IBM

Host Access Client Package V4 Update

Web Express Logon and Web Start

ZipPrint added to HOD

New PCOMM features

Byron Braswell
Ayako Nishioka
Anna ONeal
Sriram M R
AchimTepper
AchimZorn

Redbooks

ibm.com/redbooks

International Technical Support Organization

Host Access Client Package V4 Update

February 2004

SG24-6182-02

Take Note! Before using this information and the product it supports, be sure to read the general information in “Notices” on page xxi.

Third Edition (January 2004)

This edition applies to Version 4 of the Host Access Client Package, which includes IBM WebSphere Host On-Demand Version 8, Personal Communications for Windows Version 5.7.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- ibm.com®
- iSeries™
- pSeries®
- z/OS®
- zSeries®
- Advanced Peer-to-Peer Networking®
- AnyNet®
- AFP™
- AFS®
- AIX 5L™
- AIX®
- AS/400®
- CICS Connection®
- CICS®
- Domino®
- DB2 Universal Database™
- DB2®
- DPI®
- DRDA®
- GDDM®
- IBM®
- IMS™
- IMS/ESA®
- Lotus Enterprise Integrator®
- Lotus Notes®
- Lotus®
- LANDP®
- MQSeries®
- MVS™
- Netfinity®
- Notes®
- Operating System/2®
- OS/2®
- OS/390®
- OS/400®
- Redbooks™
- RACF®
- SecureWay®
- SP1®
- Tivoli Enterprise™
- Tivoli®
- VisualAge®
- VTAM®
- WebSphere®
- Redbooks (logo) ™
- IBM eserver®
- IBM eServer™

The following terms are trademarks of other companies:

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM® Redbook will help you install, configure, administer, and use the products distributed in the IBM Host Access Client Package Version 4. The package consists of:

- IBM WebSphere® Host On-Demand Version 8.0
- IBM Personal Communications for Windows Version 5.7

Many enhancements have been made in these products. This redbook covers the features and functions of Host On-Demand Version 8 and IBM Personal Communications Version 5.7 for Microsoft Windows.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Byron Braswell is a Networking Professional at the International Technical Support Organization, Raleigh Center. He received a B.S. degree in Physics and an M.S. degree in Computer Sciences from Texas A&M University. He writes extensively in the areas of networking and host integration software. Before joining the ITSO three years ago, Byron worked in IBM Learning Services Development in networking education development.

Ayako Nishioka is a Technical Support Engineer in IBM Japan Systems Engineering. Her areas of expertise include Personal Communications, Host On-Demand, and WebSphere Host Access Transformation Server. She has written extensively on Mac OS X Support and Web Start clients.

Anna O’Neal is a Software Documentation Writer for the IBM Software Group at Research Triangle Park, North Carolina. She received a M.S. degree in Technical Communication from NC State University and currently writes Host On-Demand documentation. Her areas of interest include human factors, Web design, and user interfaces.

Sriram M R is a Developer working for the IBM Software Group. He has five years of experience in software development and training field. He holds a bachelor’s degree in Computer Science from Dr. G R Damodaran College of Science. He currently maintains and develops portions of IBM Personal Communications. His interests include large scale programming, component architecture, and native OS programming.

Achim Tepper is a Senior I/T Specialist in Germany focusing on networking problems by customers in EMEA. He has 25 years of experience in customer support with IBM. His areas of expertise include Host On-Demand and Communication Server for AIX® and Linux. He has written extensively on HOD Administration and Java 2 support. He was one of the co-authors of the HACP Version 2 Redbook.

Achim Zorn is a Software Support Specialist in IBM Germany. He has 11 years of experience supporting IBM host connection products. He holds a degree in Communication Electronics from Fachhochschule Ruesselsheim. His areas of expertise include Personal Communication, Communication Server, Host On-Demand, and LANDP®.

Figure 0-1 Anna, Achim Tepper, Sriram, Byron, Ayako, Achim Zorn

Thanks to the following people for their contributions to this project:

Margaret Ticknor
Gail Christensen
Linda Robinson
Tamikia Barrow
International Technical Support Organization, Raleigh

Sherrie Abshire
David Adcox
Shirish Amin
Bobby Barnes

Russel Blocher
Bob Bogardus
Angie Boone
Carol Carson
Alan Cohen
Casey Cooley
Charlotte Davis
Serguei Fastovets
Justin I Gause
Jon Gellin
Tom Ireton
Susan Kirkman
Sherri Midyette
Steve Modena
Jenny Nicholson
Ki H Park
Tom Poe
Jim Quigley
Tami Takamiya
Robin Yehle
Yan Zhao
IBM Research Triangle Park, NC

Thomas Domin
Arun K Janardhanan
Supriya Kannery
Sankara S Muthukrishnan
Mallanagouda B Patil
Shanker P Perumal
Harshavardhana M Puttamadaiah
Shashikanth Rao
Priyadarshini Sampath
Vinaya Sathyanarayana
Srinivasan Sivaraman
Premkumar Swaminathan
Venugopala K Vemula
A special thanks to Anandha S Srinivasan for contributing and reviewing the material
IBM Software Labs, Bangalore

Special thanks to Brian Bricker, AS400 Operations/PBX Manager at Teris L.L.C.

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

`ibm.com/redbooks/residencies.html`

Comments welcome

Your comments are important to us!

We want our IBM Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  `ibm.com/redbooks`

- Send your comments in an Internet note to:

  `redbook@us.ibm.com`

- Mail your comments to the address on page ii.

1

Introduction to the Host Access Client Package

The IBM Host Access Client Package is a solution for all of your host connection needs. The package provides:

- Access to applications and data on IBM @server iSeries (5250), IBM @server zSeries (3270), and DEC/UNIX virtual terminal (VT) hosts for traditional Web users in SNA and intranet environments
- Thin client technology to distribute host access capability to remote users, as well as users in intranet and extranet environments
- The ability to create new graphical user interfaces to front-end host information without programming, using drag and drop technology

The IBM Host Access Client Package offering integrates WebSphere Host On-Demand and IBM Personal Communications into a single packaged solution. This package can provide access to legacy applications to virtually any type of user regardless of their needs. Whether it is an office-based power user, a mobile employee, a systems programmer, or a business partner with no training on host applications, the Host Access Client Package fits virtually any user need. With the addition of relatively simple graphical rejuvenation tools, you can make your applications easy to use and available to virtually anyone, virtually anywhere.

IBM Host Access Client Package offers a migration path from traditional emulation to Web browser-based emulation, with the ability to put a simple graphical user interface on a host application. This bundle focuses on TN5250, TN3270E, and VT applications support.

The components of this package are:

- IBM WebSphere Host On-Demand Version 8.0

  Host On-Demand provides Java applets that enable host connectivity and terminal emulation for 3270, 5250, and VT displays, plus FTP, and JDBC access, using industry-standard TCP/IP protocols for communications to the host. The Java applets are downloaded from a Web server through a Web browser.

- IBM Personal Communications Version 5.7

  Personal Communications provides host connectivity and emulation for Telnet 3270, Telnet 5250, and VT displays; supports SNA applications and technologies and TCP/IP.

Note that the Screen Customizer product available in previous releases of Host Access Client Package is no longer available.

1.1 Host On-Demand

WebSphere Host On-Demand is targeted to customers who wish to provide easy, and cost-effective host access with security to users in intranet-based and extranet-based environments. It enables businesses to extend the reach of their host applications and data to new users, including business partners, suppliers, and sales personnel.

Host On-Demand gives users secure browser access to host applications and data, with Web browser-based emulation. With support for TN3270E, TN5250, VT and CICS® applications included in a single package, users need to learn only one interface to reach key host data. Because Host On-Demand is Java based, users in different operating environments get the same look and feel, and identical feature set.

Host On-Demand is installed only on the Web server, and the Host On-Demand applet is downloaded through a Web URL to the user's Web browser. Code maintenance, updates and configurations all occur on the Web server, and users are updated automatically. The Host On-Demand cached client reduces download and user idle time, enhances productivity, and helps save significant expense in product deployment and maintenance.

Host On-Demand can be installed on nearly any server platform to fit nearly any size organization or branch office. Host On-Demand is supported by your choice of platforms, ranging from Windows NT, Windows 2000, AIX and Linux servers to iSeries™ and zSeries® mainframes. And, this benefit extends to the desktop as well. Because the interface is Java based, it is the same in every workstation environment, whether it be Windows 95, Windows NT, Windows XP, OS/2®, Linux or other supported workstation environments.

A rich Java tool set, including Host Access Beans for Java and the application programming interface (API), can enable customers to rapidly create custom e-business applications to achieve a competitive advantage. Because Host On-Demand is part of the WebSphere family, applications developed using the tool set can be incorporated into other WebSphere software projects, helping preserve your Host On-Demand investment and helping provide a quick start to the Web and e-business.

Host On-Demand is recommended for installations that require low-cost centralized deployment, easy, centralized administration, and support for a broad range of client and server platforms. IBM Personal Communications is recommended for full-function emulation, more extensive APIs and a wider range of protocols or connectivity, including APPN and other SNA technologies.

1.1.1 Host On-Demand features

The features and functions that Host On-Demand provides have been increasing steadily with each new version. It is a very powerful terminal emulator, FTP client and database-access utility, all implemented in Java and downloadable through a standard Web browser.

Features summary

Here is a summary of the main features followed by a list of features by release that have been added.

- TN3270, TN5250 and VT (VT52/VT100/VT220/VT320/VT420) emulation and a CICS Gateway client
- 3270 host printer emulation
- Database On-Demand for database query
- 3270 file transfer with MVS™, VM, CICS
- File transfer with OS/400®
- File Transfer Protocol (FTP) and Secure Shell FTP (sftp) client
- Keyboard remap
- Color remap
- Copy, cut and paste
- Print screen
- Macro record/play, with prompts and waits and a powerful editor
- Session security, through the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols
- Support for firewalls
- Server-based management of user configurations
- Telnet redirection
- Host Access Class Library (HACL) for development of network-computing applications
- Host Access Beans for Java for application development
- Translation into 20 languages, with keyboard and code page support for 20 more, including Arabic, Hebrew and Thai
- Comprehensive problem determination capability
- 26 sessions allowed
- Ability to create customized clients
- Locally installed client on Windows machines

Host On-Demand Version 8

The main emphasis in Version 8 is on accessing host systems and host applications without user ID and password and running Host On-Demand without a browser.

- Security

  - Web Express Logon is a new feature of Host On-Demand V8 that provides an automated way for users to log on to hosts and host-based applications without having to provide an additional ID. It is designed to function within a wide range of computing environments. Web Express Logon works in conjunction with your existing network security application and does not require client certificates. See Chapter 15, “Express Logon” on page 555.
  - Secure Shell (SSH) is a popular protocol for running secure sessions over a non-secure transport layer. It can be thought of as a secure replacement for Telnet and uses a different daemon (sshd instead of telnetd). Host On-Demand now supports secure VT Display sessions and secure file transfer protocol (sftp) sessions using SSH. There is no 3270 or 5250 session support. See 11.5, “Host On-Demand SSH support” on page 433.
  - The Host On-Demand File Transfer Protocol (FTP) client now provides Transport Layer Protocol (TLS) and Secure Socket Layer (SSL) based secure file transfer. This is referred to as secure FTP. The FTP server must also support secure FTP. See “FTP/sftp session” on page 322.
- Technology
  - Java Web Start is a technology which makes it possible for Java applications to be distributed over the network. Unlike applets, which must be accessed with a browser and depend on the browser JVM, Java Web Start runs as a Java application, independently of any browser. The Host On-Demand Web Start client is new Java 2 technology that provides the ability to run Host On-Demand clients without a browser. The Web Start client can eliminate some of the problems that occur when running HOD in a browser, such as inadvertently closing the browser when a session is active. See Chapter 16, “Web Start” on page 591.
  - Host On-Demand 3270 Display sessions now support the TN3270E protocol (TN3270E extensions). TN3270E is an enhanced form of the TN3270 protocol that allows users to specify an LU or LU pool to which the session will connect. TN3270E also supports the Network Virtual Terminal (NVT) protocol for connecting to servers in ASCII mode (for example, in order to log on to a firewall). HOD also supports the contention-resolution mode feature of TN3270E. This feature allows the 3270 host to indicate to the client when the host has finished updating the application screen. See “3270/5250 Connection selection” on page 280.
  - Internet Protocol Version 6 (IPv6) is the next generation of the Internet Protocol. IPv6 expands the number of available Internet addresses and provides improvements over IPv4 in the areas of routing and network configuration. Host On-Demand support for IPv6 requires Java 1.4 or later. HOD supports IPv6 on Solaris Version 8 and later, and Linux kernel 2.1.2 and later. See 2.2.13, “Support for Internet Protocol Version 6” on page 29.

  - Host On-Demand emulator and database clients now support Mac OS X client. See 5.2, “Mac OS X clients” on page 159.
  - Host On-Demand offers several improvements in the Java 2 cached client. These improvements raise the Java 2 cached client to the same level of user-friendliness and flexibility as the Java 1 cached client. See 5.9.3, “Improvements to the cached client for Java 2” on page 181.
  - Programmable Host On-Demand is a set of Java APIs that allows developers to integrate various pieces of the Host On-Demand client code, such as terminals, menus, and toolbars, into their own custom Java applications and applets. The API gives the developer complete control over the Host On-Demand desktop (what the user sees) without starting with the Host Access JavaBeans found in the Toolkit. The underlying Host On-Demand code handles all the “wiring” of the various components, including saving user preferences, such as macros, keyboard remappings, and color remappings, to the local file system for future use. The developer must only determine the layout of the Host On-Demand desktop. For more information, see *IBM Programmable Host On-Demand Reference,* SC31-6380, or on the Host On-Demand product disk, go to:

    ```
    file>///{cdrom:]/doc/en/doc/proghod/phReference.html
    ```

  - For 5250 Display sessions, Host On-Demand now supports iSeries hosts that send Unicode data using tagged Coded Character Set Identifier (CCSID) fields. This capability is supported by OS/400 V5R2. This enhancement allows Unicode data to be displayed in 5250 Display sessions. Host On-Demand supports CCSIDs 13488 (0x34B0) and 17584 (0x44B0). For more information, see the online help.

- Productivity
  - The Host On-Demand ZipPrint feature allows you to automatically print some types of 3270 documents in their entirety by making a single selection. ZipPrint is a parameterized macro that is built “on the fly” to print screen data. This ZipPrint capability is similar to the ZipPrint functions in IBM Personal Communications. See 21.9, “ZipPrint” on page 750 for more information.
  - Administrators and users can share and reuse macros, keyboard definitions and toolbar definitions from one session to the next. This increases productivity because administrators no longer need to reconfigure these components for each individual session or HTML file. Users can share a single component definition across sessions. See Chapter 23, “Sharing and reusing objects” on page 815.
  - New macro enhancements and capabilities are now available. Macros can invoke methods in Java classes (Java classes as variable types). In addition, you can print screens or a series of screens using new print

  actions that have been added. These print actions invoke the new PD3270 bean.

  - Server macro library support allows administrators to create a library (or libraries) of macros (files) on the Host On-Demand server. A macro in the library is then distributed to the user only when the user uses the macro. The Host Sessions window of the Deployment Wizard allows you to deploy server macro libraries to selected sessions from either a Web server or a shared network drive. This eliminates the need to import large macros into a session, and macros can be updated without modifying the HOD sessions or HTML definitions. See 23.1, “Overview” on page 816 and 23.5, “Scenario using server macro libraries” on page 834.
  - The Redirector now provides connection logging and allows connections to remain active during a period of inactivity. You can specify the amount of time to wait before dropping an inactive Redirector connection. See the Host On-Demand V8 Readme for Redirector scalability recommendations. For additional Redirector scalability recommendations, see

    http://www-3.ibm.com/software/webservers/hostondemand/library/v8infocenter/hod/en/help/2tabcontents.html
  - Directory Utility (DirUtil) adds a list function to its other actions, all calculated to save time by allowing management of configuration data in a batch mode environment. With this new function you can perform searches on users and groups, using criteria with flexible wildcard options. The list function writes search results to output files that can be reused as input for other actions. See 7.7.2, “The Directory Utility list action” on page 360.

- Usability
  - On most session types, you can specify up to two backup servers in addition to the main server. If you specify backup servers, then the Host On-Demand client automatically tries to connect with the backup servers if the connection with the main server fails. See “3270/5250 backup servers selection” on page 287.
  - CICS Gateway clients can now be customized more according to the needs of the user’s work habits. Users can either specify which CICS transaction starts upon host connection, or choose to begin their sessions without an initial transaction. See 5.6, “CICS Gateway client” on page 167, and “CICS Gateway client” on page 320.

For a list of all functions and enhancements, see the online *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301 documentation:

- On the CD:

```
http://[cdrom]/doc/[language]/doc/install/install.html
http://[cdrom]/doc/[language]/doc/install/install.pdf
```

- On Windows:

  Click **Start** -> **Programs** -> **IBM Host On-Demand** -> **InfoCenter** -> ***IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*.**

- On disk:

  ```
  http://[published directory]/[language]/install/install.html
  ```

For the latest information about Host On-Demand, visit the Web site at:

`http://www.ibm.com/software/webservers/hostondemand`

To subscribe to the Software Support Bulletin, go to:

`http://www.ibm.com/software/network/support`

To use the Web online Host On-Demand InfoCenter, go to:

`http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/hod/en/help/2tabcontents.html`

For a list of enhancements included in previous releases of Host On-Demand, see *IBM Host Access Client Package Update*, SG24-6182-01.

1.1.2 Host On-Demand components

Host On-Demand consists of the following components:

- One or more Web servers
- A Java environment, provided by a Java Virtual Machine (JVM)
- The Host On-Demand Service Manager
- A Web application server (optional)
- Clients
- Deployment Wizard
- Certificate management utilities
- Host Access Class Library for Java
- Host Access Beans for Java

Web servers

Since the Host On-Demand applet must be downloaded from a server to the client, a Web server must be installed on the same machine as the Host On-Demand server. Any Web server will work; we have not yet found a Web server that does not work.

On OS/400, Windows, AIX, Linux, Solaris and HP-UX, the Host On-Demand installation program will detect and configure most Web servers. Configuration consists of creating the required alias for the Host On-Demand publish directory so that the applet and other files are available to clients.

The client code is available for download once Host On-Demand is installed and the Web server configured. If the configuration server model is used (see 13.1, "Host On-Demand configuration models" on page 502), then the Host On-Demand Service Manager is utilized to configure and manage users and sessions.

Java Virtual Machine

Since Host On-Demand consists of a set of Java applets and applications, a Java environment is required on both the server and the client. This Java environment is provided by a Java Virtual Machine (JVM).

The Java Virtual Machine is installed along with the Host On-Demand code. Host On-Demand V8 installs the IBM 1.3.1, 1.4.0 or 1.4.1 JVM, depending of your server platform. For all other servers the JVM must be obtained and installed separately.

Clients are supported on Java 2-enabled Web browsers, such as Netscape 6.x and Mozilla. The Java 2 Plug-in with Netscape 4.x and Microsoft Internet Explorer is also supported. For more information refer to 5.16, "Web browsers: Java 1 and Java 2 enabled" on page 213.

Host On-Demand Service Manager

The Host On-Demand Service Manager consists of multiple sub-functions each of which is discussed in detail in Part 1, "IBM WebSphere Host On-Demand" on page 19.

- Configuration server

  The configuration server centrally stores and manages session configuration data and user preferences by user and group IDs. The configuration server is managed using the Administrative client.

- Redirector service

  The Redirector is a Telnet proxy that may be used to protect internal Telnet servers and ports from Internet users or to provide security for Telnet servers that do not support security natively.

- OS/400 Proxy

  The OS/400 Proxy is a proxy that allows clients to connect to a back-end AS/400® system through a single port, instead of exposing the address and ports of the AS/400 to end users.

- Configuration servlet

  The Configuration Servlet is very useful in Internet environments. The servlet runs under control of a Web application server and is configured to relay communications between the client and configuration server over standard HTTP(S) connections.

- Native Authentication

  This is a function that is used to authenticate Host On-Demand defined users with the native operating system of the server upon which the Host On-Demand server is running. This is supported only on Windows NT, Windows 2000, Windows XP, AIX, OS/390® and z/OS® operating systems.

Web application server

A Web application server, such as IBM WebSphere Application Server V4 or V5, Lotus® Domino® R6, or iPlanet Application Server V6 is required to run the Configuration Servlet.

Clients

Host On-Demand provides several types of pre-configured clients. Note that an emulator client can support all of the listed terminal types from a single full-function client.

- Emulator clients
  - 3270 display
  - 3270 print
  - 5250 display
  - 5250 print
  - VT
- FTP client
- Database clients
- Administrative clients
- Utility clients

Host On-Demand provides these full-function clients as either a cached client or as a download client, or both, with normal or debug options. In addition, the Deployment Wizard utility allows for the creation of custom emulation clients.

All available clients are explained in detail in Chapter 5, “Clients” on page 149.

Deployment Wizard

The Deployment Wizard is a utility that allows the administrator to build an emulation client customized for their environment. By using the Deployment Wizard to build custom clients, the administrator can affect the size of the downloaded or cached client, restrict the client to a subset of functions that they may perform, and establish the security capabilities of the client. The list below is a partial list of the capabilities of the Deployment Wizard.

- Type(s) of emulation allowed:
  - 3270 display
  - 3270 print
  - 5250 display
  - 5250 print
  - VT
  - CICS Gateway client
  - FTP
- Capabilities of the emulator:
  - Keyboard remap
  - Color remap
  - File transfer
  - Macro play/record
- Cached or download client
- Normal or debug options
- User model
  - Configuration Server
  - HTML-based
- Portlet creation

For a complete discussion of the Deployment Wizard, refer to Chapter 14, “Deployment Wizard” on page 517.

Certificate management utilities

The certificate management utilities are installed on Windows and AIX platforms during installation. These applications provide the capability of managing digital certificates and keyring files used by the Host On-Demand clients and Redirector on supported platforms. Refer to Chapter 12, “Certificate management” on page 473 for additional information.

Host Access Class Library for Java

The Host Access Class Library (HACL) for Java, delivered on the Host On-Demand Toolkit CD, provides a set of classes and methods that allow the development of platform-independent applications that can access host information at the data stream level. HACL implements the host access function in a complete class model that is independent of any graphical display and requires only a Java-enabled browser or comparable Java environment.

With HACL, application developers can write Java applets that manipulate data from the data stream presentation space (such as 3270, 5250, and VT) without requiring that the applets reside on the client machines.

HACL is a significant improvement over traditional emulator programming interfaces, such as EHLLAPI, in several respects. It is an object-oriented API, with all the well-known benefits of the object-oriented programming paradigm and it requires far fewer statements to achieve the same result.

For more details, refer to Chapter 24, “Host Access Toolkit” on page 843.

Host Access Beans for Java

The Host Access Beans for Java provide emulator functions as a set of JavaBeans. JavaBeans are components that have configurable properties that use events to communicate between each other, and that can be manipulated in visual development environments. The Host Access Beans can be used by developers to rapidly develop custom applications that deliver the specific functions they want to include in their host-access applications.

For more details, refer to Chapter 24, “Host Access Toolkit” on page 843.

Screen Customizer default graphical interface

Host On-Demand has the ability to automatically render the classic “green screen” into a basic graphical user interface. A default graphical user interface, Screen Customizer/LE, is included in all the Host On-Demand clients and can be turned on in the session configuration panels, but this cannot be customized. The IBM Screen Customizer product is no longer available separately or as part of the Host Access Client Package product.

1.1.3 Architecture and operations

Figure 1-1 illustrates the basic operations of Host On-Demand. We briefly describe the components and how Host On-Demand works, referring the reader to more specific chapters.

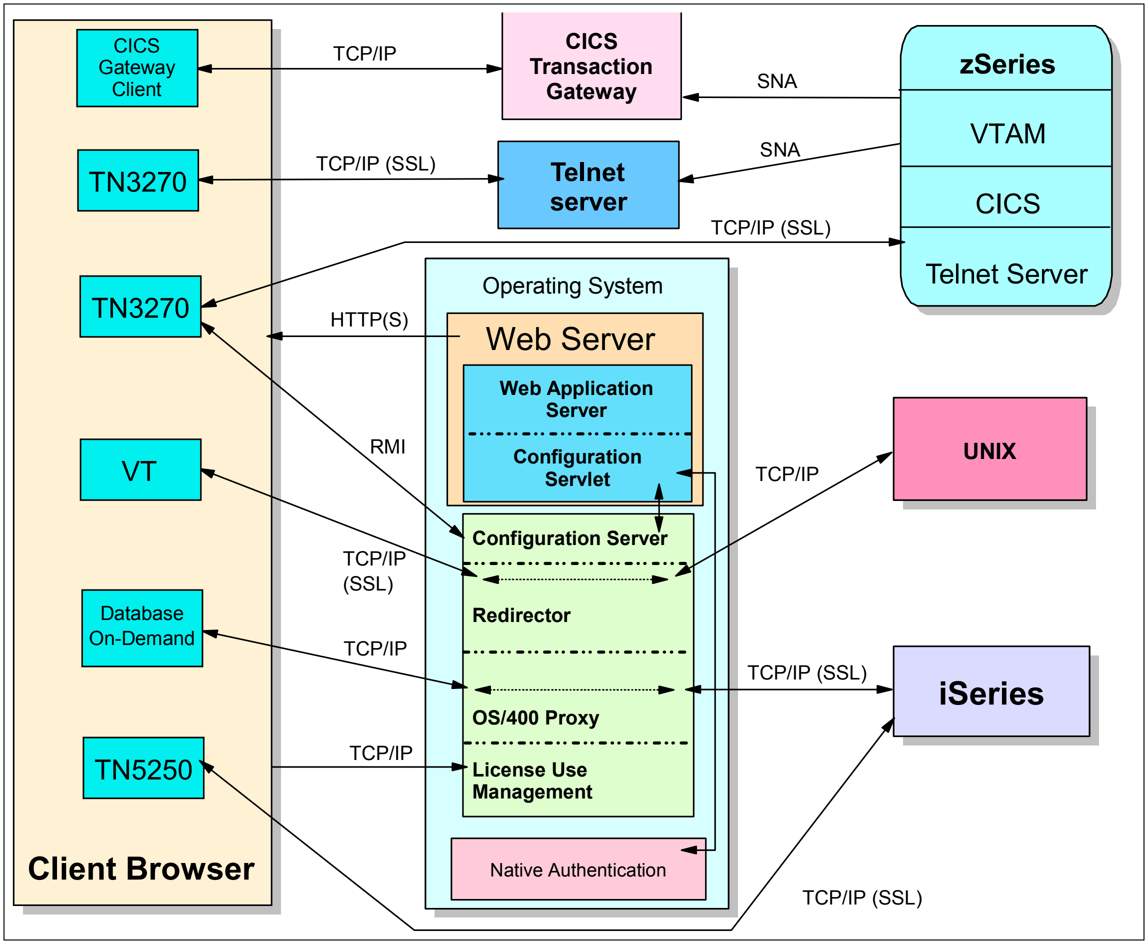


Figure 1-1 Host On-Demand basic operations

Host On-Demand is installed on a Web serving platform. This platform can be almost any platform that supports a Web server, and Java.

A client browser running a Java Virtual Machine contacts the Web server and requests an HTML page that has a Host On-Demand client embedded. This connection to the Web server may optionally be secured with HTTPS.

Configuration information for the client is either downloaded with the HTML page or is obtained from the Host On-Demand configuration server component through a non-secure TCP RMI connection using port 8999 by default. To secure this configuration information and to simplify administration in an Internet environment with firewalls, a Configuration Servlet running under a Web application server can be configured and HTTP(S) used to pass the configuration information as opposed to the non-secure RMI connection.

If configuration information is obtained from the Host On-Demand configuration server and not through the HTML files, then the ability to store these preferences using Windows user IDs is supported. Additionally, the ability is provided to challenge the user for their user ID and password as known by the server upon which Host Access Client Package is running.

Once the configuration information is obtained, any of the clients shown in Figure 1-1 may be invoked by the user in the following ways:

- Connections are supported to the CICS Transaction Gateway using the CICS Gateway client on a non-secure TCP/IP connection
- Standard TN3270(E) and TN5250 connections are supported to any of the following:
  - Stand-alone Telnet servers through secure or non-secure connections
  - Host On-Demand Redirectors
  - Communications Server for AIX Redirectors through secure, non-secure, or passthrough connection
  - Direct to an iSeries or zSeries server through secure or non-secure Telnet protocols
- VT sessions are supported in the following ways:
  - Directly to a supported VT host through non-secure Telnet connections
  - To a Redirector through a secure Telnet connection that can then connect to the back-end non-secure VT host
- Database On-Demand connections to an iSeries host in the following ways:
  - Direct to the iSeries through secure or non-secure TCP/IP connections
  - Through the Host On-Demand OS/400 Proxy through a non-secure TCP/IP connection

In order to provide the administrator a mechanism for insuring that the company stays within its licensing agreement, the License Use Management function is provided on the Host On-Demand server. This function, when enabled, provides a count of the maximum number of users concurrently running a Host On-Demand client at any given point in time.

This architecture and operations is fully described in Part 1, “IBM WebSphere Host On-Demand” on page 19.

1.2 Introduction to Personal Communications

Host Access Client Package V4 ships with Personal Communications Version 5.7 for Windows. Personal Communications Version 5.7 is Windows XP certified and runs on Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, and Windows XP. Both products are market leaders for traditional client access and connectivity, providing connectivity and APIs for all environments.

Personal Communications brings the power of personal networking to your workstation by exploiting networking capabilities to provide a variety of connectivity options supporting local area network (LAN) and wide area network (WAN) environments. Whether it is for host terminal emulation, client and server applications, or connectivity, Personal Communications offers a robust set of communication, networking, and administrative features.

Personal Communications is a full-function emulator. In addition to host terminal emulation, it provides these useful features:

- File transfer
- Dynamic configuration
- An easy-to-use graphical interface
- APIs for SNA-based client applications
- An API allowing TCP/IP-based applications to communicate over an SNA-based network

A variety of SNA-based client application programming interfaces (APIs) are supported by Personal Communications. You can create applications that use the peer-to-peer client APIs, which are based on LU 6.2 and provided by Personal Communications. These APIs let you simultaneously access and process information on peer workstations.

Personal Communications supports Advanced-Peer-to-Peer Networking (APPN) as an end node, and uses the advanced network features: high-performance routing (HPR) and dependent LU requester (DLUR).

AnyNet® SNA over TCP/IP is a feature of Personal Communications that allows emulator, and client and server SNA applications to communicate over a TCP/IP network.

Enterprise Extender (HPR over IP) allows you to extend the reach of SNA applications and data to include IP networks and IP-attached clients with similar levels of reliability, scalability, and control as SNA users. Personal Communications supports the Enterprise Extender (EE) Data Link Control (DLC).

Refer to Part 2, “Personal Communications Version 5.7” on page 915 for more information.

1.3 National Language Support

IBM, as a true international leader of global information technology, has a global vision for all its products. As a part of its globalization strategy, IBM ensures all its products, communications, and services are designed to meet the needs of the global market.

This means that they must support the language, culture, and character encoding elements of IBM’s worldwide customers. The strategy is to do this in a consistent and comprehensive manner, and at the same time leveraging existing international standards where possible.

National Language Support (NLS) provides a standardized method of supporting multiple international locales, code pages, input methods, sort orders, and number, currency, time, and date formats.

1.3.1 The need for National Language Support

As the global economy becomes more integrated, users require software compatibility across multicultural and multilingual barriers. They want to run applications using their own language and local conventions for time display, menu selections, and error messages.

A large corporation with several branches offices around the world may require that its applications to have interfaces for more than one language, such as a mixture of English, Japanese, and French software environments with perhaps multiple languages supported in a single site.

Enterprises with such complex requirements require a unified system-software architecture that can support global networks without the incompatibilities often found with different localized versions of software. Not only do they require unified system-administration models and policies, but they also need to be able to develop internal applications that operate without modification across all their operations.

For an application to be successful and to reach the global marketplace, it has to be made in accordance to the local customs, conventions, and other requirements. These could be culturally specific, such as the way the date is represented and how decimals are rounded.

In accordance with the IBM globalization strategy for its products, the Host Access Client Package is translated to several languages to ensure its global reach. The individual products such as Host On-Demand and Personal Communications Version 5.7 are provided in many languages. The session windows, configuration panels, help files, and the documentation have been translated. In addition, display, keyboard, and processing support is provided for Arabic, Hebrew, Thai, Hindi, and Greek.

The languages and code pages supported by Host On-Demand are listed in the National Language Support section of the online *Planning, Installation, and Configuring Host On-Demand*. There is also a list of the suffixes required if you want to load non-native versions of the client applets.

Support in terms of code pages, fonts, screens, and keyboard functions have been included for a host of languages such as Arabic, Hebrew, Hindi, and Thai, as well as for the Euro, the new currency of the European Union. For a complete and comprehensive list of supported languages and their levels of support, please refer to the installation guide provided along with the software.

Note: National Language Support is operating-system dependent. It calls for the availability of the necessary font and keyboard support for the language you want to use, and it should be installed in the operating system. For example, if you want to use French as the host-session language but do not have the French font and keyboard support installed, you may not be able to display the correct characters.

1.3.2 Globalization demystified

This section attempts to explain some of the technical terms and jargon used:

National Language Support Supporting multiple international locales, code pages, and input methods to a software product using a standards based approach that makes the software product culturally correct and closer to the user.

Internationalization The process of designing software applications so that it can be adapted to various languages and regions without engineering changes. Sometimes the term internationalization is abbreviated as i18n, because there are 18 letters between the first “i” and the last “n.”

Localization The process of adapting software for a specific region or language by adding locale-specific components and translating text. The term localization is often abbreviated as l10n, because there are 10 letters between the “l” and the “n.” Usually, the most time-consuming portion of the localization phase is the translation of text. Other types of data, such as sounds and images, may require localization if they are culturally sensitive. Localizers also verify that the formatting of dates, numbers, and currencies conforms to local requirements.

DBCS Double-Byte Character Set, which is used in Asia Pacific countries, including Japan, Korea, Taiwan (Traditional Chinese), China (Simplified Chinese), and Hong Kong (Simplified Chinese). As the name suggests, it may be assumed that DBCS simply means a character-encoding scheme where each character occupies two bytes. However, depending on the scheme such as EBCDIC, ASCII, ISO2022, and Unicode, each character could occupy one or more bytes in the DBCS environment.

Code Page (CP) A code page (CP) is the specification of code points (hexadecimal value) for each character in a character set. Each CP has its own ID number. For example, Japanese Katakana has a Code Page ID number 930.

Unicode Provides a unique number for every character, irrespective of the platform, or program or language.

1.3.3 Installation

When you install any or all the products of the Host Access Client Package on a Windows server or on an iSeries, you can choose which languages you wish to be installed.

Part 1

IBM WebSphere Host On-Demand

In this part, we review Host On-Demand Version 8.0. We address all aspects of the product from installation planning to deployment strategies, from administration to client operations, and migration issues from prior versions of Host On-Demand.

2

Planning and installation

This chapter discusses the planning for an installation of Host On-Demand on all platforms except zSeries. Installation on this platform is significantly different from installation on distributed platforms; therefore, we will discuss zSeries planning and installation in Chapter 3, “z/OS implementation” on page 69.

2.1 Supported platforms

The following sections describe the Host On-Demand server and client requirements for supported platforms. Additional sections cover installation and migration considerations for supported platforms.

2.2 Server requirements

In the following sections, we will examine the server requirements.

2.2.1 zSeries platform

For a complete list of OS/390 and z/OS requirements, see the Program Directory that comes with the media.

2.2.2 iSeries platform

Table 2-1 iSeries server requirements

Server operating system	OS/400 (R) V5R1 and V5R2. Recent cumulative service is recommended. Recent cumulative service is recommended. Refer to for service information: http://www-912.ibm.com/s_dir/slkbase.nsf/recommendedfixes Unicode support using Coded Character Set Identifiers (CCSIDs) requires V5R2 with the following PTFs: SI08903, SI08904, SI08933 and SI08985
Disk space	363 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Memory	256 MB memory or more. Refer to http://publib.boulder.ibm.com/pubs/html/as400/onlinelib.htm for additional information about the impact of additional memory and Java performance
Supported Web servers	► Apache-based HTTP Server for iSeries ► IBM HTTP Server for iSeries ► Lotus Domino for iSeries (manual configuration required)

Java	IBM Java Toolbox Java Developer's Kit *BASE option and one of the following: - Option 4 - 1.1.8 - Option 5 - 1.3 - Option 6 - 1.4
All other requirements	- TCP/IP Connectivity Utilities for iSeries - QShell Interpreter

2.2.3 Microsoft Windows platforms

Table 2-2 Windows server requirements

Server operating systems	► Windows NT 4.0 with SP5 or later ► Windows 2000 Professional, Server and Advanced Server ► Windows XP Professional (32-bit) ► Windows server 2003
Disk space	363 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Supported Web servers (automatically configured)	► Apache HTTP Server V1.3 and V2.0 ► IBM HTTP Server V1.3.12.6, V1.3.19.2, V1.3.26, and V2.0.42 ► iPlanet Web Server Enterprise Edition V6.0 ► Lotus Domino R6 (manual configuration required) ► Lotus Go V4.6 ► Microsoft IIS 4, 5, 5.1, and 6
Supported Web Application Servers	► iPlanet Application Server V6.0 (manual configuration of servlet required) ► Lotus Domino R6 (manual configuration of servlet required) ► WebSphere Application Server 4.0, 5.0, and 5.0 Express
Java	Installed with Host On-Demand

2.2.4 AIX platform

Table 2-3 AIX server requirements

Server operating system	AIX (R) Version 4.3.3, 5L, 5.1 and 5.2
Disk space (installp image)	363 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed (including the additional security files).
Supported Web servers	▸ Apache HTTP Server V1.3 and V2.0 ▸ IBM HTTP Server V1.3.12.6, V1.3.19.2, V1.3.26, and V2.0.42 ▸ iPlanet Web Server Enterprise Edition V6.0 ▸ Lotus Domino R6 (manual configuration required) ▸ Lotus Go V4.6
Supported Web Application Servers	▸ iPlanet Application Server V6.0 (manual configuration of servlet required) ▸ Lotus Domino R6 (manual configuration of servlet required) ▸ WebSphere Application Server 4.0 and 5.0
Java	Installed with Host On-Demand

2.2.5 Solaris platform

Table 2-4 Solaris server requirements

Server operating system	Sun Solaris 7, 8, and 9
Disk space	363 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Supported Web servers	▸ Apache HTTP Server V1.3 and V2.0 ▸ IBM HTTP Server V1.3.12.6, V1.3.19.2, V1.3.26, and V2.0.42 ▸ iPlanet Web Server Enterprise Edition V6.0 ▸ Lotus Domino R6 (manual configuration required) ▸ Lotus Go V4.6

Supported Web Application Servers	► iPlanet Application Server V6.0 (manual configuration of servlet required) ► Lotus Domino R6 (manual configuration of servlet required) ► WebSphere Application Server 4.0 and 5.0
Java	Installed with Host On-Demand

2.2.6 HP-UX platform

Table 2-5 HP-UX server requirements

Server operating system	11.0 and 11i
Disk space	363 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Supported Web servers	► Apache HTTP Server V1.3 and V2.0 ► IBM HTTP Server V1.3.12.6, V1.3.19.2, V1.3.26, and V2.0.42 ► iPlanet Web Server Enterprise Edition V6.0 ► Lotus Domino R6 (manual configuration required) ► Lotus Go V4.6
Supported Web Application Servers	► iPlanet Application Server V6.0 (manual configuration of servlet required) ► Lotus Domino R6 (manual configuration of servlet required) ► WebSphere Application Server 4.0 and 5.0
Java	Installed with Host On-Demand

2.2.7 Linux and other UNIX platforms

Table 2-6 Linux server requirements

Server operating system	► Red Hat Linux 7.1, 7.2, 7.3, Red Hat Enterprise Linux AS 2.1, 8.0 Personal, 8.0 Professional, 9.0 Personal, and 9.0 Professional ► SuSE Linux 7.1, 7.2, 7.3, 8.0, 8.1 Professional, and 8.2 ► Caldera 3.1, SCO-Caldera OpenLinux Workstation 3.1.1, and SCO-Caldera OpenLinux Server 3.1.1 ► TurboLinux 6.5, 7.0, 8.0 Workstation, and 8.0 Server
Disk space	363 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Supported Web servers	► Apache HTTP Server V1.3 and V2.0 ► IBM HTTP Server V1.3.12.6, V1.3.19.2, V1.3.26, and V2.0.42 ► iPlanet Web Server Enterprise Edition V6.0 ► Lotus Domino R6 (manual configuration required) ► Lotus Go V4.6
Supported Web Application Servers	► iPlanet Application Server V6.0 (manual configuration of servlet required) ► Lotus Domino R6 (manual configuration of servlet required) ► WebSphere Application Server 4.0, 5.0, and 5.0 Express
Java	Installed with Host On-Demand

When using Redhat Linux Version 7.0, make sure that the glibc package is at least Version 2.2-12.

2.2.8 OS/2 platform

Table 2-7 OS/2 server requirements

Server operating system	► OS/2 (R) Warp Server Version 4 ► OS/2 Warp Server for e-Business 4.5
Disk space	510 MB. The hard disk must be configured for HPFS.
Supported Web servers	Lotus Domino Go Web server for OS/2
Java	OS/2 JDK 1.1.8 or JDK 1.3.

You can obtain the latest OS/2 JVM from one of the following Web sites:

```
ftp://ftp.hursley.ibm.com/pub/java/
http://www.ibm.com/developerworks/java/
```

For JVM 1.1.8, make sure your classpath entry in config.sys is updated with the location of the JVM class files and that the current directory (.) is included. The classpath should include something like this:

```
c:\Java11\lib\classes.zip;
```

Note: When you have installed the JDK and set the classpath, reboot the workstations so that the updated classpath takes effect.

2.2.9 Novell Netware platform

Table 2-8 OS/2 server requirements

Server operating system	Novell NetWare Version 4.2, 5.1 and 6
Disk space	510 MB.
Supported Web servers	Novell Web Server
Java	Novell JDK 1.1.8. and JDK 1.3

You can obtain the latest Novell JDK from: `http://www.developer.novell.com`

The JDK must be configured for long-filename support.

Note: For users to load the client HTML files from a Novell server, their browsers might need to be configured not to use a proxy server. In addition, if users have a browser with a Java 2 plug-in, the IBM plug-in must be 1.3.1 or later, and the Sun plug-in must be version 1.3.1 or later. The client applets do not successfully load if the plug-in is an earlier version.

2.2.10 Supported LDAP servers

The Host On-Demand server can optionally use the lightweight directory access protocol (LDAP) as a data store for user and group information. The following LDAP servers are supported:

- IBM LDAP Directory Server V3.2.2
- IBM Directory Server V4.1 and V5.1
- IBM LDAP Server running on OS/390 V2R9 and V2R10
- IBM LDAP Server running on z/OS V1R1, V1R2, V1R3, and V1R4
- Netscape Directory Server V4.0 (Windows NT and AIX)

For more information on IBM's LDAP Directory solution, and to download a complimentary evaluation kit, go to:

```
http://www.software.ibm.com/network/directory/
```

For instructions on using LDAP with Host On-Demand, see Chapter 18,"Configuring Host On-Demand Server to use LDAP" on page 129.

2.2.11 Development environments

Host On-Demand supports the following Development environments:

- IBM's VisualAge® for Java Version 3.5 and 4.0
- WebSphere Studio Application Developer 4.0 and 5.0
- WebSphere Studio Site Developer Advanced 4.0
- Borland/Inprise's JBuilder Version 5.0, 6.0, 7.0, and 8.0

2.2.12 Miscellaneous software

The following software is supported:

- IBM WebSphere Portal for Multiplatforms 2.1, 4.1, and 4.2
- CICS Transaction Gateway 5.0.1 (required for CICS Gateway client)
- Acrobat Reader (Acrobat) Version 4.0 or later
  (**Note**: Acrobat Version 5.0 or later is required for DBCS PDF support.)
- Netegrity Siteminder 5.5
- IBM Tivoli® Access Manager for e-business 4.1

2.2.13 Support for Internet Protocol Version 6

Internet Protocol Version 6 (IPv6) is the next generation of the Internet Protocol designed by the Internet Engineering Task Force (IETF) to replace the current version, which is now referred to as Internet Protocol Version 4 (IPv4). For almost 20 years, IPv4 has been very effective for the Internet, but now it is experiencing certain limitations. For example, the main limitation is the growing shortage of IPv4 addresses, which is a big concern as the Internet continues to grow with more and more machines needing IP addresses. IPv6 expands the number of available IP addresses and makes improvements in areas such as routing and network configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a period of transition.

Support for IPv6 requires Java 1.4. on the server (where it is installed by default) and the client.

Host On-Demand 8 supports IPv6 on the following operating systems, because only the JVM for this operating systems supports IPv6:

- Solaris Version 8 and later
- Linux kernel 2.1.2 and later (Red Hat Version 6.1 and later)

> **Note:** A Linux client may be installed with a dual IP stack that supports both versions after which the client will be able to use IPv4 to talk to the Web server and HOD server, and IPv6 to talk to the TN3270/TN5250 server.

For an up-to-date list of operating systems supported by Host On-Demand that use IPv6, visit the Host On-Demand V8 Web InfoCenter at:

`http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/`

> **Note:** To be able to use a TN3270 or TN5250 session using IPv6, the Telnet-server must also support this; for example, Communications server for z/OS V1R5.

2.3 Client requirements

For updates to client requirements, refer to the readme.html, which can be found in /HostOnDemand/HOD/*language*/doc/readme/.

2.3.1 Supported operating systems

Host On-Demand clients are supported on the following operating systems:

- Windows 95 (no local client support)
- Windows 98
- Windows Millennium Edition (ME)
- Windows NT 4.0 with SP5 or later
- Windows 2000 (Professional)
- Windows server 2003
- Windows XP Professional and Home Edition (32-bit version)
- AIX 4.3.3, AIX 5L™, 5.1 and 5.2
- OS/2 Warp 4
- Sun Solaris 7, 8 and 9
- HP-UX 11.0 and 11i
- Red Hat Linux 7.1, 7.2, 7.3, Red Hat Enterprise Linux AS 2.1, 8.0 Personal, 8.0 Professional, 9.0 Personal, and 9.0 Professional
- SuSE Linux 7.1, 7.2, 7.3, 8.0, 8.1 Professional, and 8.2
- Caldera 3.1, SCO-Caldera OpenLinux Workstation and SCO-Caldera OpenLinux Server
- TurboLinux 6.5, 7.0, 8.0 Workstation, and 8.0 Server
- Microsoft Windows NT Server 4.0 Terminal Server Edition
- Windows Terminal Services for Windows 2000
- Netstation V2R1M0
- Citrix Metaframe 1.8 for Windows Terminal Server 4.0 and 1.8 for Windows 2000 Server
- Citrix Metaframe XP Presentation Server (Versions s,a,e) for Windows
- Mac OS X 10.2.1 Host On-Demand does not support Netscape on Mac OS X.

> **Note:** A locally installed client is supported only on Windows 98, Windows Millennium, Windows NT, Windows 2000, and Windows XP.

2.3.2 Supported Web browsers

The following Web browsers are supported for you to download the Host On-Demand clients from a remote Host On-Demand server, or to run Host On-Demand on a locally installed client:

- Supported Java 1 browsers
  - Netscape Navigator 4.7

    Host On-Demand does not support Netscape on Mac OS X.
  - Netscape Navigator (OS/2) 4.61
  - Microsoft Internet Explorer 4.01, 5.01, 5.5, and 6.0 without a Java 2 plug-in installed.

> **Note:** Based on our experience during the tests, we strongly suggest that you use the latest supported browser versions, and for Microsoft Internet Explorer, the latest JVM.

Microsoft Technical Document, Q163637, available on Microsoft's Web site, provides information for Internet Explorer users on how to obtain the latest JVM for Microsoft Windows 98 operating system, Microsoft Windows 98 Second Edition operating system, Microsoft Windows Millennium Edition operating system, Microsoft Windows NT(R) 4.0 operating system, and Microsoft Windows 2000 operating systems.

For Windows XP operating system without a JVM installed, reference the Microsoft support news group for Windows XP operating system, located on Microsoft's Web site:

- Supported Java 2-enabled browsers and Java 2 plug-ins
  - Netscape Navigator 6.1, 6.2, 7.0

    Host On-Demand does not support Netscape on Mac OS X.
  - IBM Web Browser for OS/2 V1.2
  - Microsoft Internet Explorer 4.01, 5.01, 5.5, and 6.0 with a Java 2 plug-in installed.
  - Safari
  - Mozilla 1.0.2, 1.2.1

A Java-2 enabled browser requires a Java 2 plug-in. Supported Java 2 plug-ins are: Sun, IBM, and HP Java plug-ins 1.3.1, 1.4.0, and 1.4.1.

For more information about Java 2-enabled browsers and Java 2 plug-ins, refer to 5.9, “Java 2 support” on page 179.

For more the most up-to-date list of supported Web browsers, refer to the Readme and to the Host On-Demand Web site:

`http://www.ibm.com/software/webservers/hostondemand`

2.4 Installing Host On-Demand

Before installing the Host On-Demand server, ensure that you have the appropriate level of authority to access the directories, and run the commands required for installation. For example:

- On Windows, you must log in as administrator or as a user that is a member of the administrator's group.
- On OS/400, you must sign on with the QSECOFR user profile (or with another user profile with equivalent security authorities).
- On any UNIX-based operating system, you must log on with root access authority.

The Host On-Demand clients are served as Web pages, so you must install the Host On-Demand server in the same environment as an HTTP Web server. If the installation process detects one of the supported Web servers (see 2.2, "Server requirements" on page 22) is configures it automatically, otherwise, you have to do it manually after the installation has finished. The installation steps are different for each of the following operating systems:

- Installing on Windows, AIX, Linux, Solaris, and HP-UX
- Installing on OS/2
- Installing on Novell NetWare
- Installing on OS/400
- Installing on OS/390 or z/OS

2.4.1 Installing on Windows, AIX, Linux, Solaris, and HP-UX

You can install Host On-Demand:

- With a graphical interface (see "Installation using the graphical interface" on page 32).
- In console mode (see "Installation in console mode" on page 39).
- Or with a response file in silent mode (see "Installation in silent mode" on page 41).

Even if you plan to install in console or silent mode, you should read through the steps for using the graphical interface. They document environment variables required for any installation mode.

The installation is logged in hodinstall.log, which is located in the operating systems *TEMP* directory. Any deinstallation will be logged in hoduninstall.log in the same directory.

Installation using the graphical interface

The following steps guide you through the graphical interface for installation on Windows, AIX, Linux, Solaris, and HP-UX:

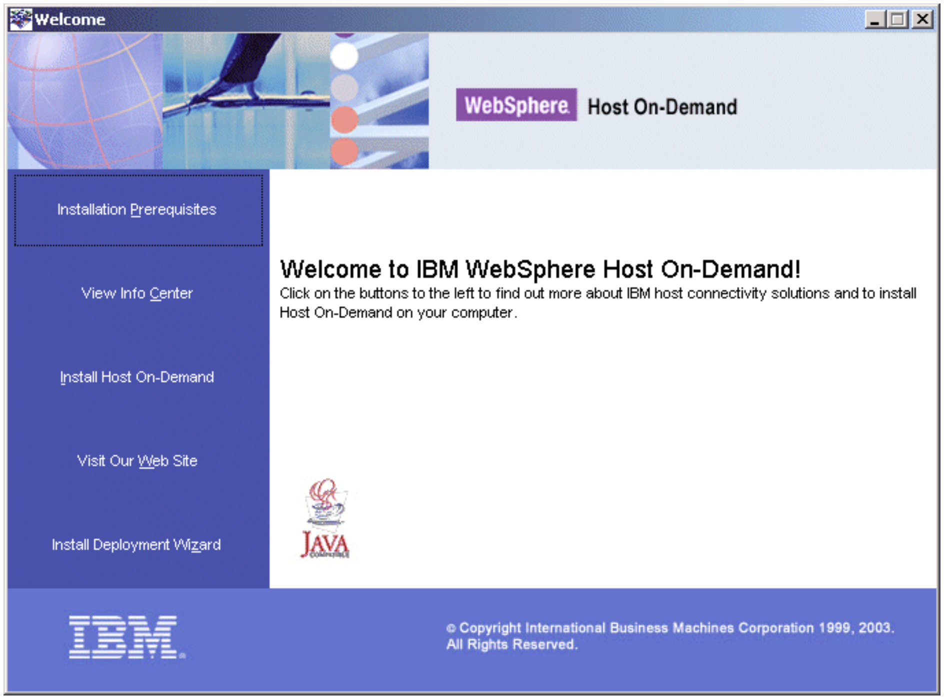
1. If your platform supports CD autoplay, insert the CD and wait for the start window. If not, you must launch the installation program with the native

platform launcher appropriate to your environment. Use one of the following (on the CD in the hodinst directory):

- hodinstallwin.exe for Windows
- hodinstallwin.console.exe for Windows. Launches the Windows console with return codes.
- hodinstall_aix.bin for AIX
- hodinstall_linux390.bin for Linux/390
- hodinstall_linuxppc.bin for Linux partitions on pSeries® and iSeries
- hodinstall_linux.bin for all other Linux versions
- hodinstall_solaris.bin for Solaris
- hodinstall_hpux11x.bin for HP-UX

As you enter your native platform launcher, you can add command-line parameters to the installation process. Refer to Appendix D in *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301 for more information.

2. The welcome window shown in Figure 2-1 appears in the language of your system or user locale.



Welcome to IBM WebSphere Host On-Demand!

Click on the buttons to the left to find out more about IBM host connectivity solutions and to install Host On-Demand on your computer.

© Copyright International Business Machines Corporation 1999, 2003. All Rights Reserved.

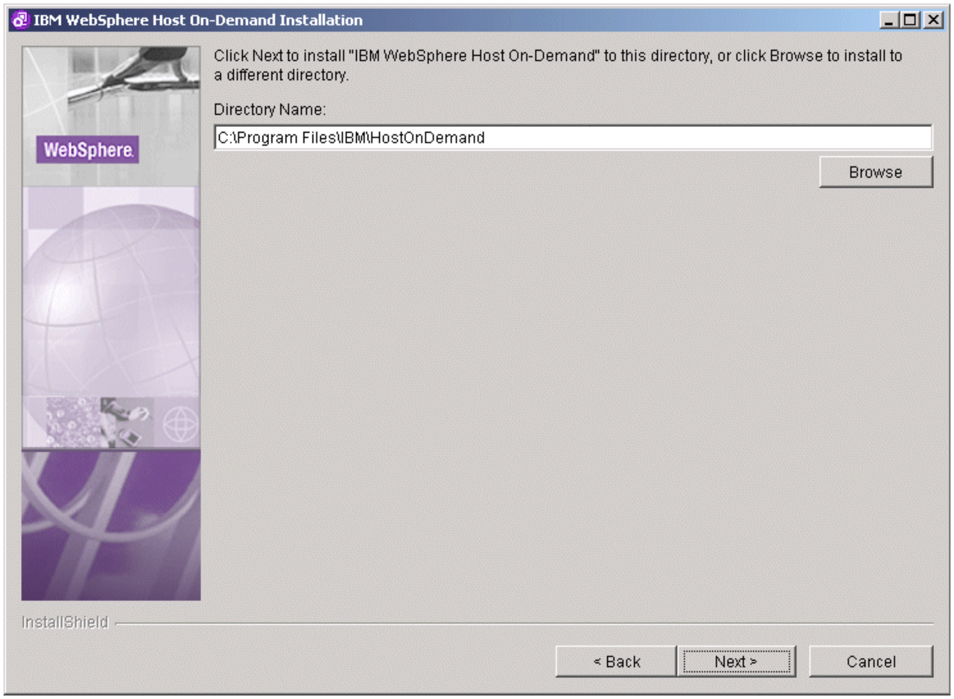
Figure 2-1 Welcome window

3. Read the software agreement, which you must accept to continue the installation.
4. If you have a previous version of Host On-Demand installed, the next window instructs you to uninstall it.

   For Host On-Demand 5, 6, or 7 on Windows and AIX, click **Next** to automatically launch the uninstall utility. It performs the uninstallation, leaving all of your existing customized HTML pages and other customized configuration files in place.

   When the utility closes, Host On-Demand 8 installation continues.
5. Next, the wizard prompts you for the installation directory. See Figure 2-2. If you are upgrading from a previous version of Host On-Demand, your previous installation directory appears as the default on Windows and AIX only. Otherwise, the installation directory defaults to one of the following:

   – c:\Program Files\IBM\HostOnDemand for Windows
   – /opt/IBM/HostOnDemand for AIX, Linux, Solaris, and HP-UX



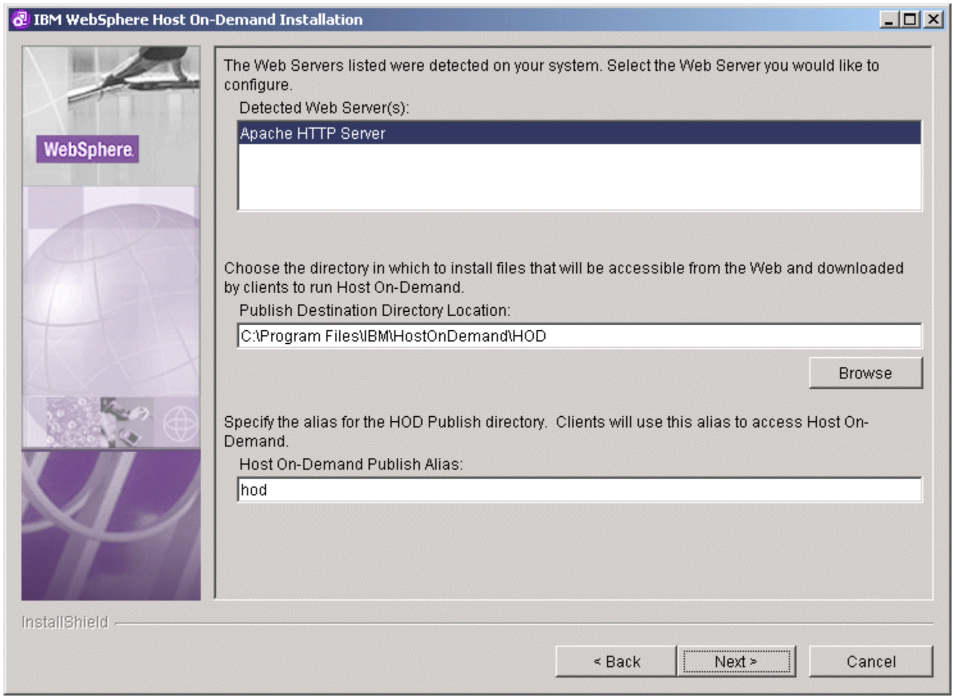
IBM WebSphere Host On-Demand Installation

Click Next to install "IBM WebSphere Host On-Demand" to this directory, or click Browse to install to a different directory.

Directory Name: C:\Program Files\IBM\HostOnDemand

Figure 2-2 Installation directory

6. The additional language selection window appears to allow you to choose support for multiple languages in addition to English, which is automatically installed.
7. The next window (shown in Figure 2-3) asks for input to configure appropriate Web servers and establish the publish directory.
   a. A list of detected Web servers appears. Select which Web server you want to configure for Host On-Demand. For a list of supported Web servers, refer to 2.2, “Server requirements” on page 22, under the platform you are trying to install on.
   b. The publish directory stores files that must be kept available to clients. The install wizard prompts you to designate your publish directory by displaying the default, HOD, as a subdirectory appended to your Host On-Demand server path. The wizard also prompts you to specify an alias for the directory.


IBM WebSphere Host On-Demand Installation

The Web Servers listed were detected on your system. Select the Web Server you would like to configure.

Detected Web Server(s):

Apache HTTP Server

Choose the directory in which to install files that will be accessible from the Web and downloaded by clients to run Host On-Demand.

Publish Destination Directory Location: C:\Program Files\IBM\HostOnDemand\HOD

Specify the alias for the HOD Publish directory. Clients will use this alias to access Host On-Demand.

Host On-Demand Publish Alias: hod

Figure 2-3 HTTP server panel

For IBM HTTP Server for Windows, the entry in the httpd.conf file will probably look like this:

```
Alias  /hod/ C:/Program Files/IBM/HostOnDemand/HOD/
```

8. Specify the Service Manager port, through which Host On-Demand clients communicate with the Service Manager. This communication is necessary for the following deployment options:

   – Using the configuration server to maintain session configuration information. See 5.1, “Host On-Demand default clients” on page 150.

   – License-Use Counting, refer to 7.6, “License Use Management” on page 353.

   IBM recommends designating port 8999 for these purposes. Check your server documentation to see if this port is being used. If it is in use, you can change the port during installation, or at a later time. For more information about changing the Service Manager port, see 2.4.6, “Changing the Service Manager port” on page 48.

9. If the installation program detects IBM WebSphere Application Server (versions 4.0 and 5.0) on your system, the next window asks if you want to

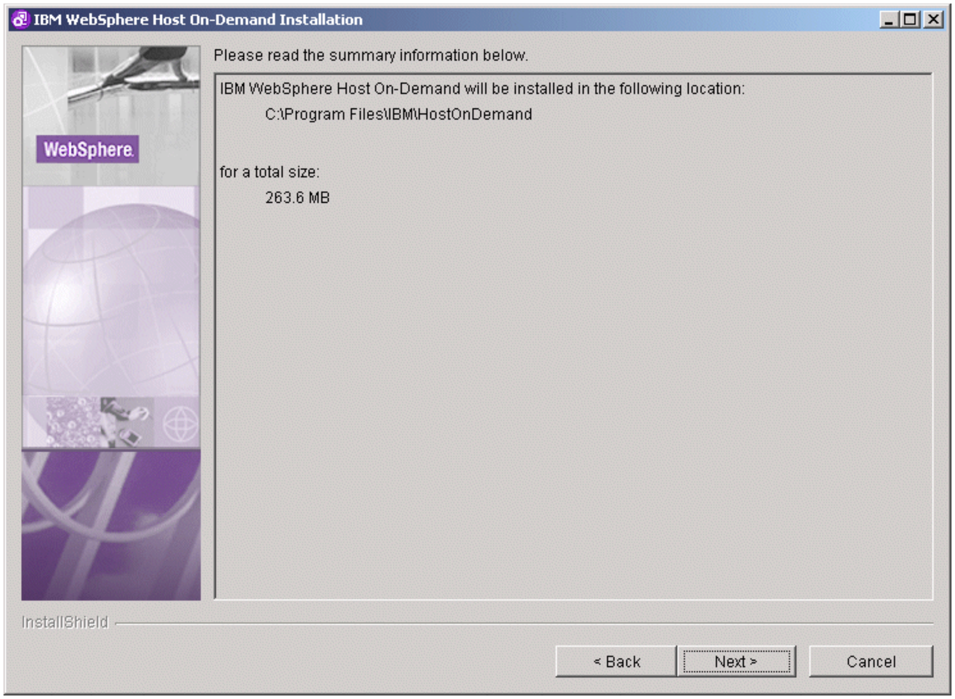
configure the Host On-Demand configuration servlet in one of them. If you run Host On-Demand through a firewall, this eliminates the need to open an extra port for client communications with the Host On-Demand Service Manager. See 2.4.7, “Installing the configuration servlet” on page 52 for more information:

- If you click **Yes,** a window appears listing the versions of the application servers detected, prompting you to choose from them. The installation program automatically deploys the configuration servlet on the Web application server you designate, and it configures your clients to access the Service Manager through the servlet.
- If you click **No**, the install configures the clients to access the Service Manager directly on port 8999 (or an alternative port you have specified).

If you click **Yes** and select **WebSphere Application Server 5**, and you have multiple servers configured within WebSphere Application Server; the install wizard prompts you to choose the server on which you want to deploy the configuration servlet.

Note: If you would like to set up your server so that some clients are using the configuration servlet and others do not, select **Yes** at this time, and refer to Chapter 9, “Configuration servlet” on page 387 for more information.

10. A window summarizing all of your input appears. This is shown in Figure 2-4. Click **Next** to install.



Please read the summary information below.

IBM WebSphere Host On-Demand will be installed in the following location:

C:\Program Files\IBM\HostOnDemand

for a total size:

263.6 MB

Figure 2-4 Summary screen

11. When the installation is complete, the wizard presents you with options to register your software and view the Host On-Demand InfoCenter.
12. When you click **Finish** in the next window, the wizard might prompt you to restart your computer.

> **Note:** For several Host On-Demand functions, the Service Manager is required to be running. On Windows servers, the Service Manager runs as a service and will be configured to start automatically at reboot. On all UNIX-based operating systems, if you reboot the server, you must also restart the Service Manager. Copy the appropriate script from /usr/opt/IBM/HostOnDemand/lib/samples/NCServiceManager/ to /usr/opt/IBM/HostOnDemand/lib/, change if needed and arrange for the script to be run at boot time. Refer to the documentation supplied with your operating system on how to add a boot service.

13. Load the HODMain.html, located in the published directory into your browser. This page contains links to all the Host On-Demand clients and utilities, the readme file, and basic configuration steps for configuring the Host On-Demand server.

Note: For AIX administrators: Be aware that installing Host On-Demand 8 on AIX results in new compiler requirements for Certificate Management. Refer to 12.4, “The IKEYCMD command-line tool” on page 493 for further information.

Installation in console mode

Installing Host On-Demand in console mode suppresses the GUI wizard. Instead, the utility sends messages and text prompts directly to your console (or command line window). You make selections by pressing the Enter key or typing a number.

To use console mode, input your native platform launcher with the -console command line option. For example, on Windows:

```
hodinstallwin.exe -console
```

When you enter the following command line options with your native platform launcher, the launcher passes them to the Host On-Demand install as installation parameters. Options that suppress the GUI wizard are marked accordingly.

Table 2-9 Command line options

Option	Purpose	Usage example
-console (Suppresses the GUI wizard)	Installs Host On-Demand in console mode.	hodinstallwin.exe -console
-log #!filename where # echoes the display to standard output and !filename is the name of the log file. If you specify ! without a file name, the default log file name is used.	Generates an installation file log with the name specified.	hodinstallwin.exe -log #!\mydirectory\logfile
-options filename	Installs Host On-Demand with command line options that set specified properties for the installation.	hodinstallwin.exe -silent -options c:\mydirectory\response File

Option	Purpose	Usage example
-options -record filename	Generates an options text file recording your responses to the Host On-Demand install wizard, establishing them as default values for installation variables.	hodinstallwin.exe -options-record responses.txt
-options-template filename	Generates an options text file containing the default installation values.	hodinstallwin.exe -options-template template.txt
-silent (Suppresses the GUI wizard)	Installs Host On-Demand in silent mode, accepting all default installation values.	hodinstallwin.exe -silent

The following additional command line options apply only to the process of calling and running the installation program. Enter them at the command line with the native platform launcher.

Table 2-10 Launch-specific command line options

Option	Purpose	Usage example
-is:logfilename	Generates a log file for the native launcher's JVM searches. hodinstallwin.exe	-is:log myLogFile.txt
-is:silent	Prevents the display of the launcher user interface (UI) while JVM searches and other initializations are taking place. (Commonly used with the command line option silent.)	hodinstallwin.exe -is:silent
-is:tempdirdirectory	Sets the temporary directory used by the Host On-Demand install.	hodinstallwin.exe -is:tempdir "c:\temp"

Installation in silent mode

A silent installation installs Host On-Demand without displaying any windows or asking for input. All of the input required during an installation is obtained from a text file called a response file. The silent mode is particularly useful for deploying multiple images of Host On-Demand server. A response file is created by recording an installation. Please refer to Figure 2-9 on page 39 for the install options to record a response file. You can find a sample response file on the Host On-Demand CD in hodinst\hodSampleResponse.txt. The defaults are English, no WebServer configuration, no WebSphere configuration, and a port value of 8999. If these values are not correct and there is not a GUI-capable console available to record a new response file, the install.script file may be copied to a writable directory and manually edited based on the comments included in the install.script file. After modifying the file for your environment, enter the following command-line options (with your native platform launcher) to run a silent installation. For example, on Windows:

```
hodinstallwin.exe -silent -options c:\mydirectory\responseFile
```

To create your own response file, you would enter the following options:

```
hodinstallwin.exe -options -record -filename c:\mydirectory\responseFile
```

Note: When you install in silent mode, there is no indication on the screen or taskbar that the installation is in progress or that it is complete. In the task manager you will find the IKERNEL.EXE running as long as the install process is active.

The directory for the response file must be defined prior to the start of the installation.

A locally installed client cannot be installed silently.

For a detailed description of the silent install process refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301. It is also available in the Infocenter shipped with Host On-Demand.

2.4.2 Installing on OS/2

Note: If you have previously installed Host On-Demand and have changed /hostondemand/private/NSMprop or changed or created /hostondemand/hod/config.properties, you must back up these files before installation and then restore them after installation. The files are overwritten during the unzip process.

The following steps assume that HostOnDemand is the server directory and `HOD` is the publish directory. To install the Host On-Demand server:

1. Insert the CD.
2. If this is a new installation, create a server directory, for example C:\HostOnDemand. The server directory contains files that are used only by the server and must not be available to client workstations
3. Change to the server directory.
4. Run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod70srv.zip
   ```

   Where:

   – `unzip` is your unpacking program (such as `UNZIP.EXE`). It must support long filenames.

   – `[cd_rom]` is the CD-ROM drive letter.

   – `zip` is the directory on the CD.
5. If this is a new installation, create the publish directory, for example C:\HostOnDemand\HOD. The publish directory contains files that must be available to client users who access the server through a browser.
6. Change to the publish directory.
7. Run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod70www.zip
   ```
8. Make the publish directory available to clients on the network. Refer to the documentation of your Web server for information about how to publish a directory.
9. Configure a local host by adding the following line to the setup.cmd file, which is usually found in the \mptn\bin directory:

   ```
   ifconfig lo 127.0.0.1
   ```
10. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application:

a. At the command prompt, change directory to \HostOnDemand\lib.

b. Copy NCServiceManager-OS2.cmd from the \HostOnDemand\lib\samples\CommandFiles directory.

c. Edit NCServiceManager-OS2.cmd to reflect the directory paths appropriate for your workstation.

d. Run **`NCServiceManager-OS2.cmd`**. The Service Manager does not display a message indicating that it has started. Also, disregard the following message: `Native library failed to load, indicating this Redirector does not support SSL`. The failure to load this library simply indicates that the server does not support SSL sessions.

> **Note:** For several Host On-Demand functions, the Service Manager is required to be running. If you reboot the server, you must also restart the Service Manager. You might want to add the **`NCServiceManager-OS2.cmd`** command to your startup.cmd file so that the Service Manager starts automatically when the workstation boots. If you do, remember to specify to change directory to /HostOnDemand/lib before running the command.

11. Restart the Web server to pick up the changes in the configuration

12. Load HODMain.html, located in the \HostOnDemand\HOD directory, into your browser:

    – Click **Readme** to see updated information.

    – Click **Basic configuration steps** to help you get started with configuring the Host On-Demand server.

2.4.3 Installing on Novell NetWare

> **Note:** If you have previously installed Host On-Demand and have changed /hostondemand/private/NSMprop or changed or created /hostondemand/hod/config.properties, you must back up these files before installation, then restore them after installation. The files are overwritten during the unzip process.

These steps assume that HostOnDemand is the server directory and HOD is the publish directory. To install the Host On-Demand server:

1. Stop the Service Manager with the **`Java -exit`** command.

2. From a client workstation, map a drive to the `SYS:` volume of the Novell server.

3. Mount the SYS:volume.
4. Insert the CD.
5. If this is a new installation, create a server directory, for example HostOnDemand. The server directory contains files that are only used by the server and must not be available to client workstations.
6. Change to the server directory.
7. From the drive mapped to the SYS:volume, run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod70srv.zip
   ```

   Where:

   – `unzip` is your unpacking program (such as UNZIP.EXE). It must support long filenames.
   – `[cd_rom]` is the CD-ROM drive letter.
   – `zip` is the directory on the CD.
8. Change to SYS:\web \docs. This directory is usually published (made available to client users who access the server through a browser) automatically. If the \web \docs directory does not exist, continue, otherwise, go to Step 10.
9. Create a publish directory named `HOD` and change to that directory. The HOD directory contains files that must be available to client users who access the Host On-Demand server through a browser.
10. Run the following command to extract the files to the publish directory:

    ```
    unzip [cd_rom]:\zip\hod70www.zip
    ```
11. From the server console, run the command **`load java`** to start the Java NLM.
12. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application, by following these steps from a client system mapped to the `SYS` volume of the server:

    a. Copy NCServiceManager-Novell.ncf from the \HostOnDemand\lib\samples\CommandFiles directory to the \system directory on the Novell server. To run the command from the server console, you might have to change the file name to the eight-dot-three format.

    b. Edit NCServiceManager-Novell.ncf (or the eight-dot-three format of the file) to reflect the directory paths that are correct for your workstation.

    c. From the server, run NCServiceManager-Novell.ncf (or the eight-dot-three format of the file). The Service Manager does not display a message indicating that it has started.

Note: For several Host On-Demand functions, the Service Manager is required to be running. If you reboot the server, you must also restart the Service Manager.

2.4.4 Installing on OS/400

There are three options for installing the Host On-Demand server on OS/400 systems:

- Using the graphical interface for remote installation (see "Using the graphical interface for remote installation" on page 45)
- Using the console or silent mode for local installation (see "Using the console or silent mode for local installation" on page 47)
- Running a remote console or silent installation from a Windows machine (see "Running a remote console or silent installation from a Windows machine" on page 48)

For information about the impact of additional memory and Java performance, refer to the iSeries Performance Capabilities Reference Web page:

http://www.ibm.com/servers/eserver/iseries/perfmgmt/resource.htm

Recent cumulative service is recommended. Refer to the Fixes, Downloads and Updates Web page:

http://techsupport.services.ibm.com/eserver/fixes

Search for iSeries.

Using the graphical interface for remote installation

To install on OS/400 in graphical mode, you must install remotely from a computer running Windows. The following steps guide you through the install:

1. Insert the Host On-Demand CD into your Windows system and open the Windows command prompt window. If your computer has CD autoplay, exit out of the Host On-Demand Welcome window.
2. At the command line prompt, change to the hodinst directory and enter the Windows launcher with an additional parameter specifying the OS/400 operating system:

   ```
   hodinstallwin.exe -os400
   ```

   Alternatively, you can use three more parameters to designate the exact server to which you are installing and log onto that server. For example:

   ```
   hodinstallwin.exe -os400 myserver myuserid mypassword
   ```

Myserver is the TCP/IP address or host name for your iSeries server. *Myuserid* and *mypassword* are a valid logon ID to that server.

3. If you do not specify the iSeries server and your logon ID in the command line, a window appears prompting you to enter that information. After you enter that information, the wizard starts. It automatically uses the language of your location, defined on your system by the running Java Virtual Machine (JVM).
4. Read the software agreement. You must accept the software agreement to continue the installation.
5. If you have a previous version of Host On-Demand installed, a window appears instructing you to uninstall it. For Host On-Demand 4, 5, 6, and 7, click **Next** to automatically delete the previous version. All of your existing customized HTML files and other customized configuration files will be saved.

   After the previous version is deleted, Host On-Demand 8 installation continues. Customized files will be restored after Host On-Demand 8 installation completes.
6. The additional language selection window appears to allow you to choose support for multiple languages in addition to English, which is automatically installed.
7. A list of Web servers detected on the iSeries system appears. Select which Web server you want to configure for Host On-Demand. For a list of supported Web servers, refer to 2.2.2, “iSeries platform” on page 22.
8. Specify the Service Manager port, through which Host On-Demand clients communicate with the Service Manager. This communication is necessary for the following deployment option:

   – Using the configuration server to maintain session configuration information (as in the configuration server-based and combined deployment models, described in Planning for deployment).

   IBM recommends designating port 8999 for these purposes. Check your server documentation to see if this port is being used. If it is in use, you can change the port during installation or at a later time. For more information about changing the Service Manager port, see *Changing the Service Manager's configuration port* in the online help.
9. If the installation program detects IBM WebSphere Application Server (versions 4.0 and 5.0) on your system, the next window asks if you want to configure the Host On-Demand configuration servlet in WebSphere Application Server. If you run Host On-Demand through a firewall, this eliminates the need to open an extra port for client communications with the Host On-Demand Service Manager. See *Installing the configuration servlet* for more information.

- If you click **Yes**, a window appears listing the versions of the application servers detected, prompting you to choose from them. The installation program automatically deploys the configuration servlet on the Web application server you designate, and it configures your clients to access the Service Manager through the servlet.
- If you click **No**, the install configures the clients to access the Service Manager directly on port 8999 (or an alternative port you have specified).

10. A window summarizing all of your input appears. Review and click **Next** to install.
11. When you see the installation complete message, click **Finish** to exit the wizard.
12. Restart the Web server using the following commands:

```
ENDTCPSVR *HTTP HTTPSVR(DEFAULT)
STRTCPSVR *HTTP HTTPSVR(DEFAULT)
```

13. If you want the Host On-Demand Service Manager to automatically start after an IPL (when `QSYSWRK` is started), type the following command:

```
CHGHTTPA AUTOSTART(*YES)
```

14. Load `http://`*`server_name`*`/hod_alias/hodmain.html` (where *server_name* is the name of your server and hod_alias is the directory you set in step 3) to verify that the Web server can serve Host On-Demand HTML pages.

For advanced configuration information, see “Configuring Host On-Demand on iSeries” in *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301. You can find this manual on the installation CD.

Using the console or silent mode for local installation

Installing Host On-Demand in console mode suppresses the GUI wizard. Instead, the utility sends messages and text prompts directly to your console (or command line window). You make selections by pressing the Enter key or typing a number.The silent mode is particularly useful for deploying multiple images of Host On-Demand server. The silent mode requires no interaction between you and the systems constituting your installation. You simply distribute a text-only response file supplying installation input.

The following steps apply to both console and silent installations on your iSeries server:

1. Place the Host On-Demand installation CD in the CD-ROM drive of your iSeries server.
2. Sign on with the QSECOFR user profile or a profile with equivalent security authorities.

3. Enter `STRQSH` at the command line to start the Qshell interpreter.
4. Enter `cd /QOPT/HOD/instmgr` to change directories to the installation CD's instmgr directory.
5. Run the following shell script according to your installation mode:

```
Console: inst400.sh
Silent: inst400.sh -silent -options/mydirectory/responseFile
```

For a description of all installation options parameters refer to Figure 2-9 on page 39.

Running a remote console or silent installation from a Windows machine

To run a remote console installation from a Windows machine, enter the following:

```
hodinstallwin.exe -os400 -console.
```

To run a remote silent installation from a Windows machine, enter the following:

```
hodinstallwin.exe -os400 myserver myuserid mypassword -silent -options
c:\mydirectory\responseFile
```

For a description of all installation options parameters, refer to Figure 2-9 on page 39.

2.4.5 Installing on OS/390 or z/OS

For instructions on installing Host On-Demand on the Linux/390 operating system, refer to 2.4.1, “Installing on Windows, AIX, Linux, Solaris, and HP-UX” on page 32.

For instructions about installing Host On-Demand on z/OS or OS/390, refer to the *Host On-Demand Program Directory* supplied with the Host On-Demand product media.

For further informations about installing Host On-Demand on OS/390 or z/OS, refer to 3.2, “Host On-Demand installation” on page 73.

2.4.6 Changing the Service Manager port

The Host On-Demand Service Manager provides support for persistent user configuration, the configuration server, error logging, and the Redirector.

During Host On-Demand installation, you have the option of specifying which port the Service Manager will use to communicate with clients. The default port is 8999.

Changes to Service Manager

You change the Service Manager port after Host On-Demand is installed by updating the `NSMprop` file. If the Service Manager is running on z/OS, see 3.3.6, “Changing the configuration port” on page 80 for details. For all other platforms, follow the instructions below to make changes to the Service Manager:

1. Stop the Service Manager:

   – On Windows systems, it runs at a service. Stop it from using the Services panel.
   – On OS/2 press CTL-C in the window from where it was started.
   – On Novell enter `java-exit` from the console.
   – On a UNIX machine use the following sequence:

   Determine the process ID of the Service Manager by entering the following command:

   ```
   ps -ef | grep NCServiceManager
   ```

   The system responds with a line similar to the following:

   ```
   root 20130 22944   0   Feb 16  pts/1  0:20 java
   com.ibm.eNetwork.HODUtil.services.admin.NCServiceManager
   /opt/IBM/HostOnDemand
   ```

   The number following root is the process ID (20130 in the example above).

   Enter `kill -9 20130` at the command prompt.

2. Change ConfigServerPort parameter

   This can be done in one of several ways. Choose the most convenient method. These are listed in order of precedence based on where the parameter is set. These parameters are case-sensitive:

   a. Add the command-line parameter `/ConfigServerPort=8999` to the end of the command you use to start the Configuration Server (or edit the script that is used to start the Configuration Server so that the ConfigServerPort parameter is passed to it).

   On the iSeries, use CFGHODSM to add the ConfigServerPort parameter.

   On Windows machines the Service Manager runs as a service so that this parameter could be entered in the registry or in the properties panel for the service, but we do not recommend this. Please refer to option b) and c).

   b. Edit the `NSMprop` file to add ConfigServerPort=8999 to the bottom of the file. The `NSMprop` file is found in the private directory of the Host On-Demand server. For example:

      - On Windows: C:\Program Files\IBM\HostOnDemand\private
      - On z/OS: /usr/lpp/HOD/hostondemand/HOD/private

   c. Edit the `NSMprop` file to update CONFIGSERVER_PARMS:

      ```
      CONFIGSERVER_PARMS = %INSTALL_PATH% 8999
      ```

      This method provides compatibility with previous versions of Host On-Demand.

3. Restart the Service Manager.

   Because there are several ways to specify a different configuration port for the Service Manager, there is a precedence that takes place based on where the parameter is set:

   a. First is a command line parameter, such as /ConfigServerPort=12345.

   b. Second is the ConfigServerPort entry in the `NSMprop` file.

   c. Third is the setting of the second parameter of CONFIGSERVER_PARMS in the `NSMprop` file.

4. Next, change the port the Host On-Demand clients use.

Changes to Host On-Demand clients

When you elect to use a port other than the default of 8999, you must notify all clients of the port change.

There are several ways to make the necessary changes to each entity, but it is important to note the order of precedence. There must be a match between the port specified for the Service Manager, the clients, and the configuration servlet (if used) in order for the clients to successfully access the Service Manager. If you have trouble accessing the Service Manager, verify each possible point of change to make sure one parameter is not canceling out another. These are listed below in the order of precedence based on where the parameter is set:

1. Change the ConfigServerPort parameter in the client HTML. The preferred method is through the Deployment Wizard. See 14.3.2, “Configuration server-based model example” on page 537 for an example. Only clients that use the customized HTML files will pick up the change. If you need to manually modify the HTML, use the PARAM tag inside the APPLET tag to set the `ConfigServerPort` parameter. For example:

   ```
   <PARAM_NAME=ConfigServerPort VALUE=8999>
   ```

2. Change the ConfigServerPort parameter in the config.properties file. This change will be picked up by all clients.

Edit config.properties to add ConfigServerPort=8999 to the file. If a config.properties file does not exist, create it and add the parameter. The config.properties file is found in the publish directory of the Host On-Demand server. For example:

- On Windows: D:\Program Files\IBM\HostOnDemand\HOD
- On z/OS: /usr/lpp/HOD/hostondemand/HOD

Example 2-1 config.properties file

```
# This file is used to set properties that apply to all Host On-Demand
# applets loaded from this directory. By default, config.properties is
# read by each applet and used to over-ride default values.
# Parameters set using HTML PARAM tags will take precedence over those
# set in this file.
# Examples:
# =========
# ConfigServer=hodserver.ibm.com
# ConfigServerPort=12345
#
# For WebSphere Application Server 3.5x
#  ConfigServerURL=http://hodserver.ibm.com/servlet/HODConfig/hod
# For WebSphere Application Server 4.x
#  ConfigServerURL=http://hodserver.ibm.com/HODConfig/HODConfig/hod
#
ConfigServerPort=8999
```

Force any active Host On-Demand clients to re-read the config.properties file by clearing your browser's cache and reloading the Host On-Demand applet.

Because there are several ways to specify a different configuration port for the clients, there is a precedence that takes place based on where the parameter is set:

- ConfigServerPort parameter set in the client HTML.
- ConfigServerPort parameter set in the config.properties file.

If you are using the configuration servlet and you change the Service Manager port, you will need to set the ConfigServerPort parameter for the configuration servlet. For example, if you change the Service Manager port to 12345, you need to pass the ConfigServerPort=12345 parameter to the configuration servlet so it can communicate with the Service Manager. Check your Web server or servlet engine documentation for information about how to pass parameters to servlets.

2.4.7 Installing the configuration servlet

During the Host On-Demand installation, you can choose to have the configuration servlet installed and configured on OS/400, Windows, AIX, Linux, Solaris, and HP-UX. A list of supported Web application servers for each platform can be found in 2.2, “Server requirements” on page 22.

Installing the configuration servlet is necessary only if both of the following statements are true for your Host On-Demand deployment:

- You plan to configure Host On-Demand so that client communication with the Service Manager is necessary (as in the configuration server-based and combined deployment models, if you enable License-Use Counting, or if you use the Redirector).
- A firewall protects the servers on which you plan to maintain session configuration information, and you do not want to open a port in that firewall to give outside clients access to the Service Manager.

By default, the Host On-Demand clients use port 8999 to access configuration information from the Service Manager. If any of your clients are outside the firewall, the firewall administrator needs to open port 8999 both internally and externally. However, you can avoid opening this port by customizing your clients to use the configuration servlet to access configuration information. If you are using the configuration servlet and you change the Service Manager port, you will need to set the ConfigServerPort parameter for the configuration servlet. For example, if you change the Service Manager port to 12345, you need to pass the ConfigServerPort=12345 parameter to the configuration servlet so it can communicate with the Service Manager. Check your Web server or servlet engine documentation for information about how to pass parameters to servlets.

All Web servers and servlet engines are configured differently. Check your Web server and servlet engine documentation for servlet configuration details on your operating system.

For a complete discussion of the configuration servlet, see Chapter 9, “Configuration servlet” on page 387. You may also want to refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301*,* and the online help.

2.4.8 Installing the locally installed client

The locally installed client installs to a local disk on the client machine. The client applet is loaded directly into the default system browser, so there is no download from a server. The most common reason to use a local client is for users who connect remotely over slow telephone lines, where download time can be an issue and connectivity is unpredictable. You can also use the locally installed client to test host access capabilities without installing the full Host On-Demand product.

Locally installed clients are supported on Windows 98, Windows Millennium, Windows NT, Windows 2000, and Windows XP. To install the Host On-Demand local client on a Windows NT, Windows 2000, or Windows XP workstation, you must be a member of the administrator's group.

1. Insert the CD and run the following command from the /hodinst directory of the CD:

   ```
   hodinstallwin.exe -lc
   ```

2. Click **Install**.
3. Proceed through the rest of the windows.
4. If you have not already done so, read the Readme available in the last window.
5. At the end of installation, the Host On-Demand Service Manager is configured and started automatically. On Windows NT, Windows 2000, and Windows XP, the Service Manager is installed as a Service; on Windows 98, and Windows Millennium (Me) it is added to the Start menu.

Starting the locally installed client

To start Host On-Demand as a client, click **Start -> Programs -> IBM Host On-Demand -> Host On-Demand**.

Removing the local client

To remove the local client, use add/remove programs from the control panel. If InstallShield does not remove the hostondemand directory, you must remove it manually.

2.4.9 Installing the Deployment Wizard

The Deployment Wizard is automatically installed as part of the Windows Host On-Demand server installation. It is also available separately for those customers who do not wish to install the entire Windows Host On-Demand server. This separate Deployment Wizard can be installed in one of two ways:

- Using the Deployment Wizard install option on the Windows Host On-Demand server installation CD
- Downloading it from the Host On-Demand server

See Chapter 14, “Deployment Wizard” on page 517, for details on using the Deployment Wizard functions.

The following two sections describe the installation process for each, respectively.

> **Note:** The Deployment Wizard installation image is approximately 85 MB. If you are planning to download this installation image, particularly over a modem, prepare for a large download.

Installing the Deployment Wizard from the Windows CD

To install and run the Deployment Wizard, do the following:

1. Insert the Host On-Demand CD. If autorun is enabled, the CD Installer starts automatically. If autorun is not enabled, start the CD Installer by running the `setupwin.exe` file located on the Host On-Demand CD.
2. From the CD Installer window, select **Install Deployment Wizard**.
3. The InstallShield Wizard will guide you through the remaining installation steps.
4. Once installation is complete, you can launch the Deployment Wizard from the **Start -> Programs** desktop menu.

Downloading the Deployment Wizard installation image from a Host On-Demand server

The Deployment Wizard image is shipped on all Host On-Demand server platforms, and can be downloaded from the server and installed on any Windows machine.

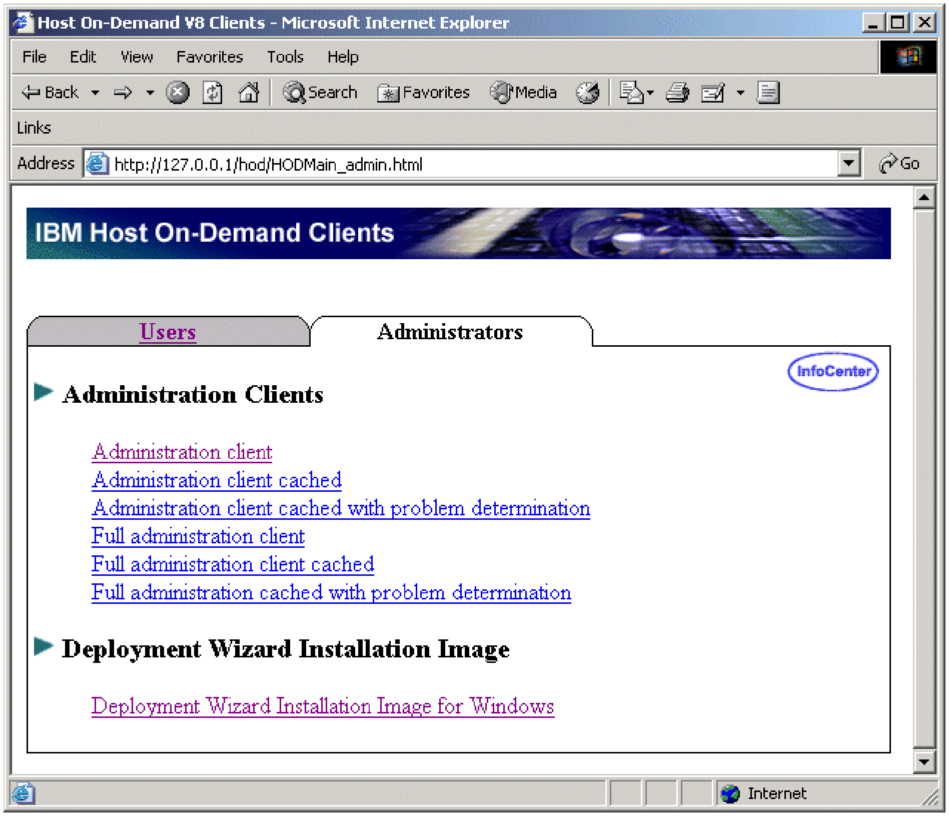
To download the Deployment Wizard from a Host On-Demand server, do the following:

1. From your Windows machine, start your browser and point to the HODMain_xx.html file on your Host On-Demand server, where xx is your two letter language suffix. You can enter and use only those languages which had

been installed on the HOD server according to Figure 2-3 on page 36. The Language suffixes are as shown in Table 2-11 on page 55.

Table 2-11 Language suffixes:

Language	Language suffix
Simplified Chinese	zh
Traditional Chinese	zh_TW
Czech	cs
Danish	da
Dutch	nl
English	en
Finnish	fi
French	fr
German	de
Greek	el
Hungarian	hu
Italian	it
Japanese	ja
Korean	ko
Norwegian	no
Polish	pl
Brazilian Portuguese	pt
Portuguese	pt_PT
Russian	ru
Slovenian	sl
Spanish	es
Swedish	sv
Turkish	tr


Host On-Demand V8 Clients - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Address http://127.0.0.1/hod/HODMain_admin.html
Go
Users
Administrators
InfoCenter
Internet

IBM Host On-Demand Clients

Administration Clients

Administration client
Administration client cached
Administration client cached with problem determination
Full administration client
Full administration client cached
Full administration cached with problem determination

Deployment Wizard Installation Image

Deployment Wizard Installation Image for Windows

Figure 2-5 Downloading the Deployment Wizard

2. Click the **Deployment Wizard** link. This will download the Deployment Wizard installation image to your Windows machine.
3. Run the Deployment Wizard installation from your Windows machine.
4. Once installation is complete, you can launch the Deployment Wizard from the **Start -> Programs** desktop menu.

2.5 Migration considerations

With very few exceptions, data used in earlier versions of Host On-Demand will be automatically migrated when you begin using Host On-Demand Version 8.

The upgrade of the Host On-Demand server is per default transparent to the clients. After the upgrade, the clients have their same sessions defined and all their customizations, for example, macros and keyboard remaps, continue to work as before (first introduced as Enhanced Local Preferences with HOD 6). On platforms where an uninstall program for Host On-Demand is not provided, the administrator must back up some files and directories before upgrading, and then restore them after the upgrade.

2.5.1 Server considerations

Any existing configuration data in your configuration server will be automatically available in Host On-Demand Version 8 once installation is complete. Even if most of the installation processes preserves any configuration data, it is recommended to back up the following data prior to installation:

- The /private directory
- All custom HTML files
- The /HODData directory
- The CustomizedCAs.class, if one exists
- NSMprop, if not default
- The NCServiceManager start script, depending on your operating system.

Table 2-12 Migration considerations

Operating system	Previous version of HOD	Migration process
Windows and AIX 4.3 or later.	5-7	Host On-Demand automatically uninstalls the previous version from your system and replaces it with Host On-Demand 8, leaving customized files intact.
Windows or AIX	previous to 5	Make sure, you have saved the above data, run the uninstall program of your installed version manually, then install HOD 8.
OS/400	4-7	Host On-Demand automatically uninstalls the previous version from your system and replaces it with Host On-Demand 8, leaving customized files intact.

Operating system	Previous version of HOD	Migration process
Any other operating system without a native uninstall utility	Does not apply	Make sure, you have saved the above data, delete the HOD directories and install HOD 8. Then restore the saved files.

Setting up a user publish directory

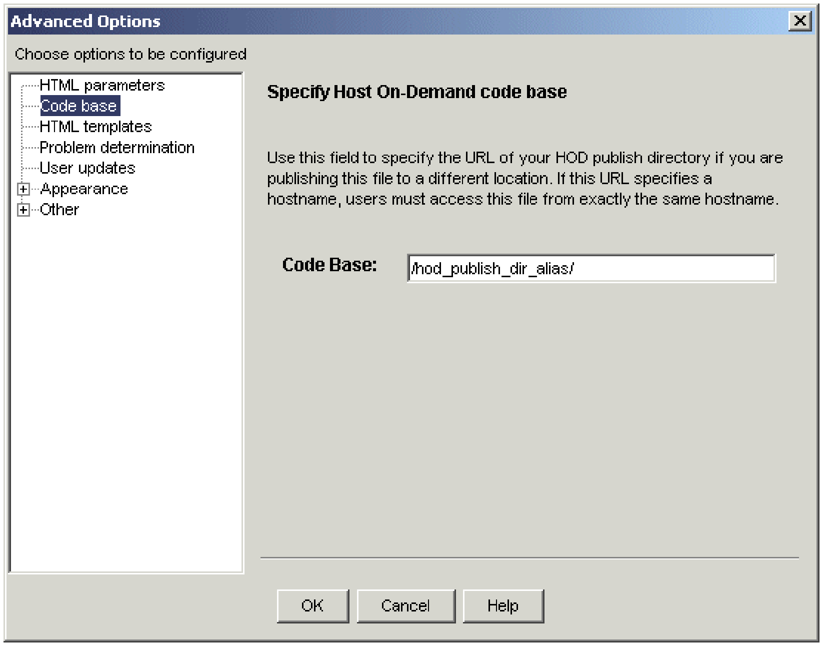
You can put custom HTML files (files generated from the Deployment Wizard), config.properties, and CustomizedCAs.p12 files in a directory other than the Host On-Demand default publish directory. Creating a user publish directory makes it easier to apply future Host On-Demand upgrades because installing a new version of Host On-Demand will not affect the new directory. It also keeps the Host On-Demand publish directory read-only and provides a separate writable location for deploying Deployment Wizard pages. Additionally, creating a separate user publish directory isolates new files from those provided by Host On-Demand. Note that other user-modified files (such as customer applets and HACL programs) still need to run from the Host On-Demand publish directory.

To set up a separate user publish directory, do the following:

1. Specify the codebase (the URL of your Host On-Demand publish directory) as follows:

   a. Using the Deployment Wizard, on the Additional Options page, click the **Advanced Options** button.

   b. Select the **Code base** selection. The window shown in Figure 2-6 will be displayed.



Specify Host On-Demand code base

Use this field to specify the URL of your HOD publish directory if you are publishing this file to a different location. If this URL specifies a hostname, users must access this file from exactly the same hostname.

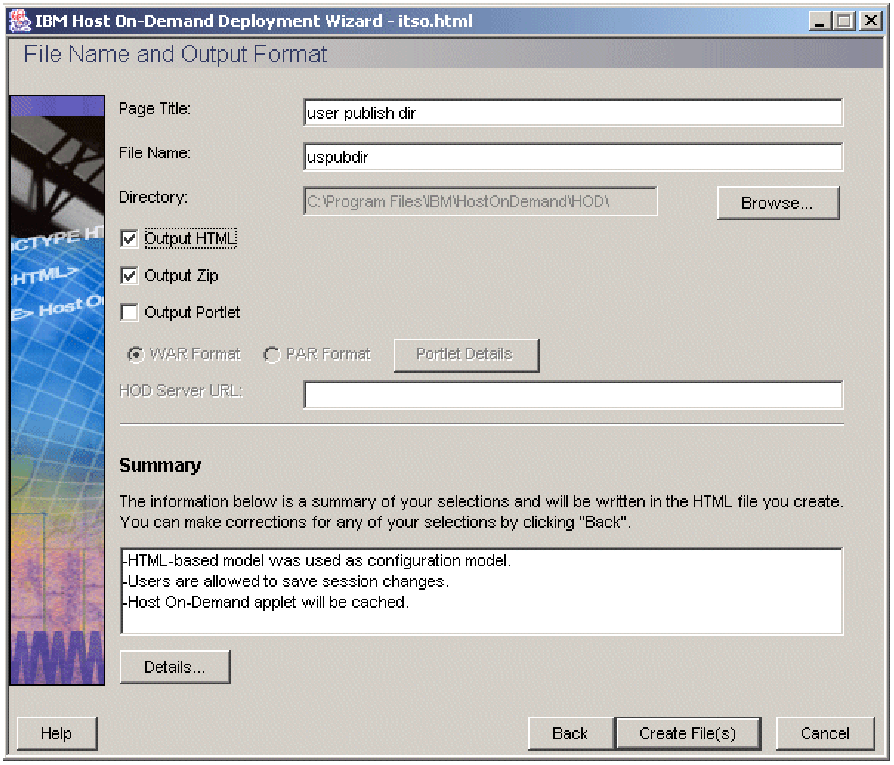
Code Base: /hod_publish_dir_alias/

Figure 2-6 Advanced Options - Code base selection

c. Enter the codebase. You can enter a fully qualified URL including the hostname (for example, `http://your_HOD_server/hod_publish_dir_alias/`) or a relative path (for example, `/hod_publish_dir_alias/`).

d. Click **OK** to return to the Additional Options window.

2. On the Additional Options page, click **Next** to proceed. The window shown in Figure 2-7 will be displayed.


IBM Host On-Demand Deployment Wizard - itso.html
File Name and Output Format

Page Title: user publish dir

File Name: uspubdir

Directory: C:\Program Files\IBM\HostOnDemand\HOD\

☑ Output HTML

☑ Output Zip

□ Output Portlet

● WAR Format ○ PAR Format

HOD Server URL:

Summary

The information below is a summary of your selections and will be written in the HTML file you create. You can make corrections for any of your selections by clicking "Back".

-HTML-based model was used as configuration model.
-Users are allowed to save session changes.
-Host On-Demand applet will be cached.

Figure 2-7 File Name and Output Format panel

3. Select **Output Zip** to save the files generated from the Deployment Wizard in HTML and a zip file format.
4. Click **Create Files**.
5. If you are not running the Deployment Wizard on your Host On-Demand server, FTP the output Zip file to your server platform.
6. Create a separate user publish directory, /user_publish_dir/.
7. Use the DWunzip tool to install the Deployment Wizard generated files into the /user_publish_dir/ directory. You must edit the DWunzip command file on your server to specify the correct `MY_PUBLISHED_DIRECTORY` value. You will find the sample `DWunzip.cmd` on Windows machines in \HostOnDemand\lib\samples\DWunzip. See the online help topic using DWunzip for more information on how to use this tool. Example 2-2 shows a simple customized section of `DWunzip.cmd`.

Example 2-2   Example of customized DWunzip.cmd

```
REM ##########################################################################
REM   If you do not use Host On-Demand's default web-published directory, then
REM   set the following variable to be your web-published directory.
REM   Note:  This is also the directory where your zip file should be.
REM   Example:   set MY_PUBLISHED_DIRECTORY=c:\HostOnDemand\HOD

set MY_PUBLISHED_DIRECTORY=c:\HostOnDemand\HOD

REM ##########################################################################
REM   If you run DWUnzip from anywhere other than the directory where
REM   Host On-Demand was installed, then set the following variable
REM   to your Host On-Demand installation directory.
REM     EXAMPLE:   set MY_HOD_DIRECTORY=c:\HostOnDemand

set MY_HOD_DIRECTORY=c:\HostOnDemand
```

The execution of the DWunzip results in Example 2-3.

Example 2-3   Execution of DWunzip

```
C:\Program Files\IBM\DeploymentWizard>dwunzip teamcom2wizz

Extracting teamcom2wizz.zip to and from directory: c:\HostOnDemand\HOD
Allocating ZIP comments array
Added ZIP comment "HODCDLABEL"
Added ZIP comment "HODCDLABEL"
Added ZIP comment "HODCDLABEL"
Added ZIP comment "HODCDLABEL"
Added ZIP comment "HODCDLABEL"
Added ZIP comment "HODCDLABEL"
File being extracted from teamcom2wizz.zip: Teamcom2wizz.html
File being extracted from teamcom2wizz.zip: HODData\Teamcom2wizz\cfg0.cf
File being extracted from teamcom2wizz.zip: HODData\Teamcom2wizz\params.txt
File being extracted from teamcom2wizz.zip: HODData\Teamcom2wizz\policy.obj
File being extracted from teamcom2wizz.zip: HODData\Teamcom2wizz\preloads.obj
File being extracted from teamcom2wizz.zip: HODData\Teamcom2wizz\wInfo.txt

File extraction was a success.
```

The Deployment Wizard HTML files are installed in the directory /user_publish_dir/. Additional files like cfg0.cf, params.txt, and so forth, are installed in the /user_publish_dir/HODData/your_html directory as shown in Example 2-3.

8. Add a pass rule (also known as an alias on some platforms) in your Web server configuration file, /etc/httpd.conf, to point to this new user publish directory. For example:

   ```
   Pass  /user_alias/*  /user_publish_dir/*
   ```

9. If changes are required in the Host On-Demand config.properties file (for example, to change the default port or enable the Host On-Demand configuration servlet), do the following:

   a. Update the config.properties file. If your server platform does not support the ASCII character set, update this file on a machine that does support ASCII.

   b. If the config.properties file was updated on a different platform than your server, FTP the file to your server platform in a binary format.

   c. Place the file in the user publish directory /user_publish_dir/.

   d. Add the following pass rule (also known as an alias on some platforms) in the Web server configuration file `/etc/httpd.conf`:

      ```
      Pass /hod_publish_dir_alias/config.properties
      /user_publish_dir/config.properties
      ```

      (All on one line)

      > **Note:** On the zSeries platform, append the ascii extension, `/user_publish_dir/config.properties.ascii.`

10. If you are using SSL and need to change the CustomizedCAs.p12 file, do the following:

    a. Place the updated file in the user publish directory /user_publish_dir/CustomizedCAs.p12

    b. Add the following pass rule (also known as an alias on some platforms) in the Web server configuration file `/etc/httpd.conf`:

       ```
       Pass /hod_publish_dir_alias/CustomizedCAs.p12
       /user_publish_dir/CustomizedCAs.p12
       ```

       (All on one line)

11. Restart the Web server.

12. From a Web browser, specify the URL: `http://your_HOD_server/user_alias/your_html.html`

Moving a Host On-Demand server installation to a new server

You can move your Host On-Demand server configuration from one server to another. If you install Host On-Demand in a test environment before deploying to your production environment, complete the following steps to migrate Host On-Demand from one server to another (or from one HFS to a different HFS in an OS/390 or z/OS environment). For example, if you wanted to move your Host On-Demand server configuration from server1 to server2, you must:

1. Install Host On-Demand on server2. You must install the same release level of Host On-Demand on server2 that is installed on server1. If server2 is using a Web server that is not recognized by the Host On-Demand installation program, you must manually configure the Web server for Host On-Demand. Refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301 for more information.
2. Stop the Host On-Demand Service Manager on server2.
3. Replace the necessary files and directories on server2 with those from server1. This step overwrites any configuration changes made to Host On-Demand on server2 since step 1.
4. Copy the \private\ directory in the Host On-Demand root directory, which is \HostOnDemand\ by default, on server1 to the \private\ directory on server2 to move user and group configuration information to server2.
5. Copy all files and directories you have created with the Deployment Wizard from their server1 location to server2. For example, if you created test.HTML using the Deployment Wizard, copy test.HTML and Autotest.HTML in the publish directory from server1 to server2. Also copy the test directory in \HODData in the publish directory from server1 to server2.
6. Start the Host On-Demand Service Manager on server2.

Note: If your current environment is not OS/390 or z/OS, and you want to move to an OS/390 or z/OS environment, this migration requires some additional steps. You can copy the private directory and CustomizeCAs.p12 file over to the new server directly. However, you should use the DWunzip utility to correctly install the customized HTML files and the /HODData directory.

2.5.2 Client considerations

There is no need to actually migrate a client, except the locally installed client. For the locally installed client, the InstallShield for Windows XP, Windows 2000, Windows NT and Windows 98 will detect any earlier version of Host On-Demand, uninstall it, and install the Host On-Demand Version 8 client.

When using a cached client, the user will be notified about the change at the server when accessing it for the first time, and any new files will be downloaded.

Upgrading HOD V4.x cached clients to HOD V8

If you upgrade your Host On-Demand server from Version 4.x to Version 8, your clients will no longer be able to communicate with the server without upgrading.

If you need to manage network demand while upgrading cached clients, you can gradually move all of your Host On-Demand Version 4.x cached clients to Host On-Demand V8 by setting up two servers. One would be a Host On-Demand Version 4.x server and the other would be a Host On-Demand V8 server. Configure all clients to access the Host On-Demand V8 server, and then add the HTML parameter HODServer to HODCached.html, or any of your customized cached client HTML files that are on the Host On-Demand V8 server. There are two sets of applet parameters defined in the HTML. Add the HODServer parameter to the set defined by the array cHod_AppletParams. You can do all of this using the Deployment Wizard on the Additional Parameters window; however, if you want to manually modify the HTML, the format for the parameter is:

```
cHod_AppletParams[7] =<PARAM NAME=HODServer
VALUE=http://yourhostname/alias/HODCached.html>
```

(All on one line)

where `yourhostname` and `alias` are your Host On-Demand Version 4.x server's hostname and alias, or publish, directory. Make sure that the index of the new cHod_AppletParams array element is in the correct sequence with the existing array elements.

The *HODServer* parameter works with the UpgradePercent and UpgradeURL parameters to manage client upgrades. If the cached client is not upgraded on this connection attempt, it is redirected automatically to the Host On-Demand Version 4.x server specified in the HODServer HTML parameter. If a cached client will be upgraded, the Host On-Demand Version 4.x cached client is removed and the Host On-Demand V8 cached client is installed. Once the client is upgraded to Host On-Demand V8, the HTML parameter is ignored and the client is no longer redirected to the Host On-Demand Version 4.x server. After you have gradually upgraded all your cached clients, you no longer need the Host On-Demand Version 4.x server.

Be aware of the following when you are upgrading cached clients from Version 4.x to Version 8:

- Cached clients are upgraded in the foreground. The upgrade in background option is ignored.

- If you have customized Host On-Demand Version 4.x HODCached.html and have called it something different, like `OurHTML.html`, do the following:
  a. Copy the Host On-Demand V8 version of HODCached.html to the file OurHTML.html.
  b. Add the HODServer parameter to OurHTML.html. The HODServer parameter should specify `http://yourhostname/alias/OurHTML.html` as the Host On-Demand Version 4.x server.
- You can copy the new HODCached.html, which includes the HODServer parameter to AutoHODCached.html and AutoHODLaunch.html in case these pages are bookmarked by the clients. `The HODServer` parameter in AutoHODCached.html should specify the AutoHODCached.html page on the Host On-Demand Version 4.x server. `The HODServer` parameter in `AutoHODLaunch.html` should specify the `AutoHODLaunch.htm`l page on the Host On-Demand Version 4.x server.
- If you are using language specific HTML files (such as `HODCached_es.html`, `AutoHODCached_es.html`, `AutoHODLaunch_es.html`, etc.) you can also add the `HODServer` to these pages.

Upgrading custom HTML files

Java 1

If your users have Java 1 browsers and you have customized HTML files from previous versions of the Deployment Wizard, you do not have to regenerate the custom files with the Host On-Demand 7 Deployment Wizard. The users can take advantage of all the new features (except Java 2-specific features) once the client code gets upgraded to Host On-Demand 8.

Java 2

If your users have Java 2 browsers, we strongly encourage you to regenerate the HTML files with the Host On-Demand V8 Deployment Wizard to receive the improved support for Java 2 environments. Additionally, if you want to take advantage of the new features built in to the Host On-Demand V8 Deployment Wizard, such as the customized template, separate codebase, or upgrade based on time of day, you should regenerate your custom HTML files.

2.5.3 Client migration problems

It is not common, but does happen that when a user upgrades a workstation from one HOD client version to another that it does not go well. For these situations you should be prepared to try the following procedures:

1. Have the user use the HodRemove.html utility to remove the existing cache client

2. Clear browser temporary cache
3. Clear Java 2 cache
4. Reload the new cache client

If this still fails to resolve the problem then use the HOD InfoCenter and refer directly to the Troubleshooting section of the Online Help. The section *client troubleshooting checklist* under the list of *Troubleshooting topics* should be very helpful.

2.6 Removing Host On-Demand

To uninstall the Host On-Demand server follow the appropriate steps for your platform.

2.6.1 zSeries

Follow the instructions in the Program Directory for uninstalling the Host On-Demand server on zSeries.

2.6.2 All other operating systems

Please refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301.

Notes:

- On Windows 2000, if you plan to reinstall Host On-Demand, you should reboot first.
- If you install the standalone Deployment Wizard on a Windows NT or Windows 2000 workstation that already has Host On-Demand server installed, you should uninstall the Deployment Wizard before you uninstall the Host On-Demand server.

  If you uninstall Host On-Demand server first, you might not be able to uninstall the Deployment Wizard because the Deployment Wizard uninstallation attempts to use the Host On-Demand JVM.

2.7 Service updates

You can access the latest information on Host On-Demand through the Support Web site. The URL is:

```
http://www.ibm.com/software/webservers/hostondemand/support.html
```

To download the latest service updates for Host On-Demand and Personal Communications, you will need to register with the IBM Software Internet Service Delivery site. The URL is:

```
http://www6.software.ibm.com/aim/home.html
```

This site entitles you to download service updates directly from the Internet. You must first register, then add your service key to your registration. The service key is the 10-digit number on the service key card that is provided for each product. Then you can download the product that matches the key you have entered. We recommend registering every key that comes in the package.

The service key must be treated with the same care given to the base product in terms of export and import regulations. It provides access through the Web to product code that contains encryption technologies. Care should be taken to read and comply with the text presented on the Authorization to Download Web page. You must agree to these terms prior to being allowed to download the product code.

Note: The service key can be used by only one person. Once registered to an individual, it cannot be registered to another individual.

When attempting to download Corrective Service Distributions (CSDs) or Program Temporary Fixes (PTFs) from the site, you must make sure that you select the product version, the language and the encryption correctly.

Please also note that this key will provide you with access to the product as long as service is generally provided for this level of code.

3

z/OS implementation

In this chapter, we discuss Host On-Demand on the z/OS platform. The base operating system referred to in this chapter is assumed to be one of the following: OS/390 V2R10 or higher, or z/OS V1.01.00 or higher. Information relevant to a particular operating system is listed. Information pertinent to both OS/390 and z/OS is referred to as z/OS. Although the z/OS environment is a UNIX environment, it is installed and maintained differently from a normal UNIX distributed environment. Therefore, this chapter will cover the following areas for z/OS, emphasizing the z/OS unique aspects:

- Planning
- Host On-Demand installation
- Activating Host On-Demand Service Manager, including the configuration of the HTTP server and RACF®
- Deployment Wizard considerations for uploading customized HTML pages, including a sample created and uploaded to a z/OS server
- Using SSL with Communications Server for z/OS, including general information about SSL on z/OS, samples of using the gskkyman certificate management utility, and RACF certificate management, TCP/IP profile for server and client authentication
- Certificate Express Logon
- Native Authentication
- LDAP directory server configuration on z/OS

3.1 Planning

Host On-Demand consists of only one FMID: *HHOJ800*.

The distribution medium for Host On-Demand Version 8 is magnetic tape. A program directory is supplied with the package, which provides the information necessary to install Host On-Demand using SMP/E, activates the Host On-Demand server, starts the Native Authentication service, and sets up the LDAP directory server.

Installing Host On-Demand by SMP/E will result in the previous Host On-Demand FMIDs being deleted, for example:

- HHOJ700 - Version 7 FMID
- HHOF600 - Version 6 FMID
- HHOH500 - Version 5 FMID

Host On-Demand on z/OS can only be installed using SMP/E. You cannot copy the .tar file from another platform and run the **`hod80mvs.sh`** shell script to install it.

It is recommended that you consult the Program Directory and the following Web sites prior to installation. Support, product information, and hints and tips can be found on the following Web sites:

- Product information site:

  `http://www.ibm.com/software/webservers/hostondemand/`

- Support site (hints and tips, service updates, newsletters):

  `http://www.ibm.com/software/webservers/hostondemand/support/`

- Program directory softcopy:

  `http://www.ibm.com/software/webservers/hostondemand/library/`

- Host On-Demand product InfoCenter and Program Directory softcopy:

  `http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/`

Maintenance for Host On-Demand V8 can be ordered in one of two ways, both of which are SMP/E installed:

- Go to the support Web site and select **Support Downloads**. You must be registered with the IBM Software Internet Service Delivery site. Refer to 2.7, “Service updates” on page 66 for additional details.
- Order the PTF tapes through IBM support.

3.1.1 Software requirements

The following prerequisites are required for the Host On-Demand V8 product to install or function:

- OS/390 V2.10.00 or higher or z/OS V1.01.00 and above:
  - If running with OS/390 V2R10 and using the LDAP directory server, maintenance (PTF UW74965, superseded by PTF UW99407) is needed to properly display LDAP sessions.
  - OS/390 or z/OS Communications Server TCP/IP services are required at runtime.
  - Java V1.3.1, V1.4.0, or V1.4.1 for OS/390 or z/OS
  - If running with OS/390 V2R10, you must install Java APAR OW45575/PTF UW78944(PTF6).
- A Web server
  - IBM HTTP Server V5.00.00 or higher (V6.00.00 supports z/OS V1.R2 and higher only)
- WebSphere Application Server if using the configuration servlet
  - WebSphere Application Server for z/OS and OS/390 V4.0.1 and higher
- For SSL encryption, one of the following elements is needed. Refer to Table 3-1 on page 92 for the correct FMID:
  - Communications Server for OS/390: IP Security SSL DES (56-bit Export)
  - Communications Server for OS/390: IP Security SSL Triple-DES (168-bit US)
- LDAP directory server (optional):
  - IBM LDAP directory server for OS/390 V2R9,R10, z/OS V1.1 or higher
  - IBM LDAP Directory Server V3.2.2

3.1.2 DASD storage requirements

DASD storage is required for the target and distribution libraries and for the Hierarchical File System (HFS). Work space is also needed during the SMP/E installation. The program directory outlines the storage requirements for Host On-Demand and for SMP/E.

The recommended space allocation is 940 MB for the distribution library, and 3500 MB for the HFS.

3.1.3 Backing up the private directory

The private directory can be backed up using either the **pax** command or the **tar** command. Assume the current private directory is for HOD V7:

1. From the Host On-Demand V7 HFS, change the directory to the private directory:

   ```
   cd /usr/lpp/HOD/hostondemand/private
   ```

2. Archive the private directory in a /tmp directory. The **-z** option compresses the file; the **-v** provides a list of files and subdirectories being archived (optional):

   ```
   pax -wzvf /tmp/private.pax.Z *
   ```

3. The private.tar.Z file was then transferred in binary to the /tmp directory on the system for Host On-Demand V8.
4. On the Host On-Demand V8 HFS, change the directory to the private directory where the file will be extracted.

   ```
   cd /usr/lpp/HOD/hostondemand/private
   ```

5. Issue the **pax** command to extract the private.pax.Z file. The **-z** option specifies a compressed file; the **-v** provides a list of files and subdirectories being extracted (optional).

   ```
   pax -rzvf /tmp/private.pax.Z
   ```

3.1.4 Upgrade considerations

When upgrading from a previous level of Host On-Demand, you will probably want to take into consideration previous customizations. The following are three processes of allocating an HFS and restoring the previous private directory. We found the third option to be the easiest:

1. Allocate a new HFS and copy the existing HFS into the new HFS. Then follow the installation procedure. The customization in the private directory will be intact. Any customizations made in any directory other than the private directory will be overwritten, so they must be backed up prior to running the **hod80mvs.sh** shell script.
2. Install into the existing HFS. With this process, you need to take into consideration space available in the HFS. Host On-Demand V8 will require more space. Any customization other than what is in the private directory will be lost as in option 1.
3. Allocate a new HFS, then follow the installation procedure. Copy your existing private directory into the new HFS using the **pax** or **tar** command. Refer to 3.1.3, “Backing up the private directory” on page 72.

With Host On-Demand V7 and later, the NSMprop file is located in the /private directory. If you have customized this file in Host On-Demand V6 or earlier, you can copy the file from the /lib directory to the Host On-Demand V8 /private directory.

Customized files not in the private directory can also be copied to the new HFS, for example: CustomizedCAs.class, CustomizedCAs.p12 (new in HOD V8), custom HTML pages, /HODData directory, and config.properties.ascii found in the publish directory.

Publish directory

With Host On-Demand V7 and later, the administrator can choose to publish files created by the Deployment Wizard to a directory other than the Host On-Demand publish directory. If you wish to move your custom HTML pages to a separate user publish directory, you will need to re-edit these files through the Deployment Wizard to add the Codebase parameter. See Chapter 14, “Deployment Wizard” on page 517 for more information on using the Deployment Wizard.

Mounting a separate user publish directory allows the administrator to mount the Host On-Demand HFS as read-only. However, when starting the ServiceManager for the first time, Host On-Demand will require write access to the /lib directory. Also, if you use the DWunzip utility you will need to either edit DWunzip-S390 prior to mounting the HFS as read-only, or copy the file to a directory with write permissions. After initialization of the ServiceManager for the first time, the Host On-Demand HFS can be changed from read and write to read-only mode. For more information on setting up a separate user publish directory, see *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301*.*

3.2 Host On-Demand installation

In this section we detail the installation of Host On-Demand on z/OS. We discuss the installation jobs and instructions, and activating and stopping the Service Manager.

3.2.1 Installation jobs

Host On-Demand can be installed into its own SMP/E environment, but sample jobs to create and initialize the environment are not provided. Sample jobs are provided to do the basic RECEIVE, APPLY, and ACCEPT functions, as well as defining the DDDEF entries.

The Program Directory provides JCL that can be used to copy the sample jobs from the product tape. Once the RECEIVE is completed, the samples can be found in the IBM.HHOJ800.F1 data set.

The sample jobs provided to install Host On-Demand V8 are:

HOMRECVE	Sample RECEIVE job
HOMALLOC	Sample job to allocate target and distribution libraries
HOMDDDEF	Sample job to define SMP/E DDDEFs
HOMHFS	Sample job to define Host On-Demand HFS data set (optional)
HOMISMKD	Sample job to invoke the supplied HOMMKDIR EXEC to allocate HFS paths
HOMAPPLY	Sample APPLY job
HOMACCPT	Sample ACCEPT job
HOMSERVR	Sample job for starting Host On-Demand

The sample jobs should be updated to reflect the CSI, target zone, and distribution zone names used in the installation.

3.2.2 Installation instructions

The program directory contains the steps for the SMP/E installation; therefore, they are not included in this book. The support Web site contains the latest program directory.

If upgrading from a previous level of Host On-Demand, you need to decide which process to follow to migrate your customization. Refer back to 3.1.4, “Upgrade considerations” on page 72. If allocating a new HFS, you may want to consider increasing the space allocation in the HOMHFS job to accommodate future service updates. Refer to 3.1.2, “DASD storage requirements” on page 71.

Create the mount point and make sure it has permissions of 755. For example:

```
TSO MKDIR ‘[PATHPREFIX]/usr/lpp/HOD’ MODE (7,5,5)
```

where [PATHPREFIX] is the appropriate high-level directory name. For users installing in the default path, this would be null. For others, the high-level directory may be something like /service/, or some meaningful name for your installation.

Note: In the UNIX System Services environment, everything is case-sensitive.

Mount the HFS to the system; it must be mounted with read and write access. This is the default if omitted on the **MOUNT** command. The command should be on one line:

```
TSO MOUNT FILESYSTEM('hfsprfx.hom.hfs')
MOUNTPOINT('[PATHPREFIX]/usr/lpp/HOD') TYPE(HFS)
```

where `hfsprfx` is the name of the qualifier used in the HOMHFS installation job.

Regardless of whether a new or existing HFS is used, you must run the HOMISMKD job to create the directory structure for the Host On-Demand product.

If you obtained Host On-Demand as part of a CBPDO, follow the installation instructions found in the CBPDO RIMLIB data set to receive the Host On-Demand FMID, HHOJ800.

Important: Depending on when the product was ordered, you may receive PTF tapes in addition to the base product tapes. You must install the base product before installing the PTF tapes. The z/OS installation requires the base to be fully installed. The **hod80mvs.sh** shell script performs tasks such as symbolic links that the PTF shell script does not.

3.3 Activating Host On-Demand Service Manager

Before you can use a Host On-Demand server, there are several steps to complete:

1. Set up the UNIX System Services environment.
2. Set up the Security Server (RACF) if you plan to run the HOMSERVR as a started task.
3. Set up the Web server environment.
4. Modify the HOMSERVR sample job to suit your environment.
5. Start the Host On-Demand Service Manager.

Note: The basic installation assumes the Host On-Demand port will be 8999, the recommended port. To change the port, refer to 3.3.6, “Changing the configuration port” on page 80.

3.3.1 UNIX System Services environment

Make sure the **LIBPATH** and **PATH** statements are all set correctly in the UNIX System Services (USS) environment. The USS file is commonly stored as /etc/profile. You need to point to your installed level of Java. You should also make sure that the LIBPATH, and PATH statements are included in the WebSphere product statements, for example /usr/lpp/internet/bin.

Note: The actual paths for Java may vary depending on your installation:

- The LIBPATH environment variable should point to the correct Java library:

  ```
  LIBPATH=/usr/lpp/java/IBM/J1.3/lib
  ```

- The PATH environment variable should point to the correct Java library:

  ```
  PATH=/usr/lpp/java/IBM/J1.3/bin
  ```

3.3.2 Security Server (RACF) considerations

The HOMSERVR sample job is supplied to start Host On-Demand. It runs the **ServiceManager.sh** shell script, which starts the Host On-Demand Service Manager (NCServiceManager).

The HOMSERVR procedure must be started from a user ID with root authority in z/OS UNIX System Services. Our examples are for z/OS RACF. Here are the basic instructions to enable Host On-Demand to be assigned to the appropriate user ID:

1. Create a user ID for the HOMSERVR procedure (for example, HOMSRV):
   a. Choose a default group that is defined to z/OS UNIX (for example, it has a z/OS UNIX segment with a group identification number (GID) defined. You might have a group called OMVSGRP that includes all z/OS UNIX users).
   b. Add a z/OS UNIX segment, giving the user ID root authority by assigning it a user identification number (UID) of 0.
2. Create a started class entry (or update ICHRIN03) for the HOMSERVR procedure:
   a. Make the entry name procname.* (for example, `HOMSRV.*`).
   b. Assign =MEMBER to the user, thereby making the user ID and the procname the same (for example, `HOMSRV.*`).

c. Assign the procname to the z/OS UNIX group that is the default group for the user (for example, OMVSGRP).

Here is an example:

Associate the Host On-Demand Started Task with a RACF user ID that has an OMVS segment defined:

```
RDEFINE STARTED HOMSRV STDATA(USER(TCPIPOE))
SETROPTS RACLIST(STARTED) REFRESH
```

where `TCPIPOE` is the user name with which the started task is associated.

If you want to create a different user ID to be used with Host On-Demand, issue the following commands:

```
ADDUSER HODSRV OMVS(HOME('/') UID(777))
          DFLTGRP(OMVSGRP) AUTHORITY(CREATE) UACC(ALTER)
RDEFINE STARTED HOMSRV STDATA(USER(HODSRV))
SETROPTS RACLIST(STARTED) REFRESH
```

Remember that the GROUP also has to have an OMVS segment defined.

3.3.3 HTTP server environment

To activate the Host On-Demand functions, the HTTP server must be configured to allow the HTML pages, class files, Web Start files, and JavaScript files to be downloaded to the user's machine. The name of the HTTP server configuration file is `/etc/httpd.conf` and it contains the configuration statements called *directives*.

The `Pass` directive specifies a template for requests that you want to be passed from the server. These Pass rules must be in the order listed in Example 3-1 and be placed prior to the ending Pass rule, `Pass /*.` The rules assume an alias of /hod/. The Web Start feature of Host On-Demand V8 requires an additional Pass directive to support Web Start clients. The first Pass directive shown in Example 3-1 is required for Web Start support.

Example 3-1 z/OS Web server Pass statements

```
Pass /hod/*.jnlp /usr/lpp/HOD/hostondemand/HOD/*.jnlp.ascii
Pass /hod/*.html /usr/lpp/HOD/hostondemand/HOD/*.html.ascii
Pass /hod/*.HTML /usr/lpp/HOD/hostondemand/HOD/*.HTML.ascii
Pass /hod/*.js /usr/lpp/HOD/hostondemand/HOD/*.js.ascii
Pass /hod/*.properties /usr/lpp/HOD/hostondemand/HOD/hod/*.properties.ascii
Pass /hod/*.props /usr/lpp/HOD/hostondemand/HOD/*.props.ascii
Pass /hod/* /usr/lpp/HOD/hostondemand/HOD/*
```

If you are using a directory path other than /usr/lpp/HOD, change the directory path to the correct path, for example, /service/usr/lpp/HOD. Keep in mind that the alias is also case-sensitive. Consult the Web Server documentation for details.

Data type directives must be added among the other rules in the AddType section of the /etc/httpd.conf file. A new AddType directive is required to support the Web Start client in Host On-Demand V8. It is the first AddType shown in Example 3-2. The other AddType directives were added in previous release of HOD.

Example 3-2 z/OS Web server AddType statements

```
AddType .jnlp application/x-java-jnlp-file 8bit 1.0
AddType .cab application/octet-stream binary 1.0
AddType .jar multipart/x-zip binary 1.0
```

If you are using a directory path other than /usr/lpp/HOD, change the directory path to the correct path, for example /service/usr/lpp/HOD.

If you wish to publish your custom HTML pages from a separate user publish directory, you will need to add a pass rule pointing the alias to your separate publish directory:

```
Pass /user_alias/* /user_publish_dir/*
```

For example:

```
Pass /hodpages/* /var/hod/customHTML/*
```

In this example, the user_alias is hodpages and our customized files will be stored in the directory /var/hod/customHTML.

3.3.4 Modify the HOMSERVR sample job

To start the Service Manager with a started task, copy HOMSERVR sample procedure to a PROCLIB known to the system, and make the necessary changes to your installation. In this example we renamed the sample HOMSERVR procedure to HODSRV. If you have a different path structure for the Host On-Demand HFS, make the change in the PARM field. If you need to direct the STDOUT and STDERR to a file, you can modify the JCL like the following example to redirect the output to a temporary file.

Example 3-3 Sample Host On-Demand started procedure

```
//HODSRV  PROC
//*
//*  Function: IBM WebSphere Host On-Demand Server JCL
//*
//HODSRV    EXEC PGM=BPXBATCH,REGION=OK,TIME=NOLIMIT,
//    PARM='sh /usr/lpp/HOD/hostondemand/lib/ServiceManager.sh'
//SYSPRINT DD SYSOUT=*
//SYSIN    DD DUMMY
//SYSERR   DD SYSOUT=*
//STDOUT   DD PATH='/tmp/homservr-stdout',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//STDERR   DD PATH='/tmp/homservr-stderr',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//SYSOUT   DD SYSOUT=*
```

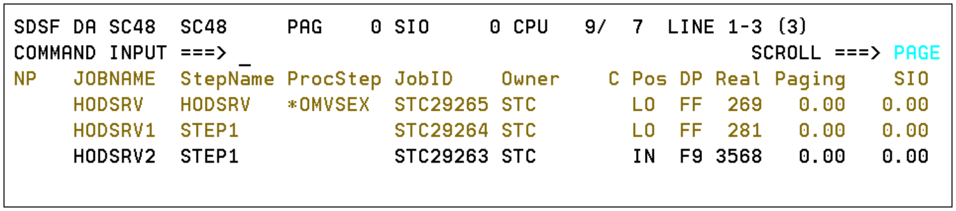
3.3.5 Start the Host On-Demand Service Manager

The Service Manager can be started one of two ways, either as a started task using the HOMSRV job or by entering the shell script from the OMVS shell. You cannot start it from the ISHELL because the environment variables set in `/etc/profile` will not be used.

To start from the z/OS console using the sample procedure defined in Example 3-3, enter:

```
s hodsrv
```

In this example the started task name, HODSRV, is less than eight characters, hence, job names HODSRVx and HODSRVy will also be created, where x and y is a numeric between 1 and 9. In this scenario HODSRV1 and HODSRV2 were created as shown in Figure 3-1. If the started task name is eight characters, all three job names will be the same.



```
SDSF DA SC48  SC48     PAG    0 SIO     0 CPU    9/   7  LINE 1-3 (3)
COMMAND INPUT ===> _                                     SCROLL ===> PAGE
NP    JOBNAME  StepName ProcStep JobID    Owner    C Pos DP Real Paging    SIO
      HODSRV   HODSRV   *OMVSEX  STC29265 STC        LO  FF  269   0.00   0.00
      HODSRV1  STEP1             STC29264 STC        LO  FF  281   0.00   0.00
      HODSRV2  STEP1             STC29263 STC        IN  F9 3568   0.00   0.00
```

Figure 3-1 Job names

From the OMVS shell, there are a couple of ways to start the Service Manager:

```
/usr/lpp/HOD/hostondemand/lib/ServiceManager.sh &
```

or

```
cd /usr/lpp/HOD/hostondemand/lib
ServiceManager.sh &
```

Remember to include the & in order to run the shell script in the background; otherwise the ID will be unusable.

Once the Service Manager is started you will get the following message in STDOUT:

```
RDR0008: Native library failed to load, indicating this Redirector does not
support SSL.
```

The message is self-explanatory and can be ignored. If you would like to eliminate the message, edit the NSMprop file in the private library, /usr/lpp/HOD/hostondemand/private. Change the following parameter from YES to NO:

```
REDIRECTOR_AUTOSTART = NO
```

The Service Manager will need to be stopped and restarted to pick up the change.

3.3.6 Changing the configuration port

To change the configuration port for Host On-Demand on z/OS, the port must be specified in two places:

1. The NSMprop file, found in the /hostondemand/private directory, sets properties for the server. This file is in EBCDIC and does not need to be downloaded to be edited. Edit the NSMprop file and change the port number in the following line found in the CONFIGSERVER section. For our example we changed the port from 8999 to 8900:

   ```
   CONFIGSERVER_PARMS = %INSTALL_PATH% 8900
   ```

2. The config.properties.ascii file sets the port for the clients. The file resides in the publish directory. Host On-Demand on z/OS ships with a config.properties.ascii file located in a subdirectory in the publish directory, /usr/lpp/HOD/hostondemand/HOD/hod. You need to edit the file on an ASCII based system. Add the following to set the port to 8900:

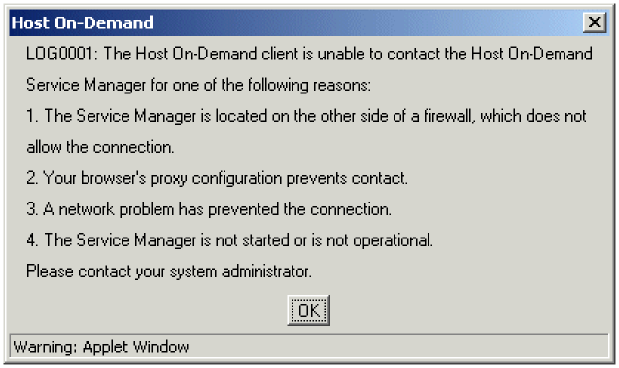
   ```
   ConfigServerPort=8900
   ```

   Then transfer the file to the z/OS server in binary. The reason for this is that the client applets expect ASCII text in config.properties.ascii, but files created or edited on z/OS are stored in EBCDIC.

After these changes have been made, the Service Manager can be started. To verify the correct port is listening, issue the TCP/IP **netstat conn** command:

To verify the client is making requests on the new port, access HODAdmin.html.

If you receive the message window shown in Figure 3-2, verify that you have transferred the file in binary mode from the workstation, and that the filename is config.properties.ascii.



LOG0001: The Host On-Demand client is unable to contact the Host On-Demand Service Manager for one of the following reasons:

1. The Service Manager is located on the other side of a firewall, which does not allow the connection.
2. Your browser's proxy configuration prevents contact.
3. A network problem has prevented the connection.
4. The Service Manager is not started or is not operational.

Please contact your system administrator.

Warning: Applet Window

Figure 3-2 LOG0001 error window

Migration concern

If your existing Host On-Demand configuration was using a port other than 8999, you must be careful during migration. During the install process, the files in the private directory are unchanged, including the config.properties.ascii file. Also, in Host On-Demand V8 the NSMprop file is installed in the directory, /usr/lpp/HOD/hostondemand/private. Therefore, you must edit the file to change the ConfigServerPort parameter to indicate the port you wish to use. For more migration concerns refer to 2.5, “Migration considerations” on page 56.

3.3.7 Stopping the Service Manager

If the Service Manager was started as a started task, the task cannot be stopped with the **purge** command as it will not work; the **cancel** command must be used. If the task name is HODSRV, stop it with the z/OS command:

```
C HODSRV
```

Note that you do not need to cancel the additional two jobs created by the system as these will be stopped when the main task is cancelled. It is recommended to use a started task name less than eight characters. If the started task name is eight characters, to cancel the Service Manager you will need to specify the ASID of the main task on the cancel command.

Important: If the level of Java on the z/OS is J1.3.1, when the cancel command is issued, CEEDUMP and HPITRACE files are created in the Host On-Demand /lib directory. If these files are not removed, eventually the HFS will become full. You can manually remove these files or add the **rm** command to the **ServiceManager.sh** script as shown in Example 3-4. Note that if you stop Host On-Demand by killing the USS process these files will not be created.

Example 3-4 ServiceManager.sh with rm command

```
rm /usr/lpp/HOD/hostondemand/lib/CEEDUMP*
rm /usr/lpp/HOD/hostondemand/lib/HPITRACE*
```

If the Service Manager was started from the OMVS shell, you need to determine the PID of the Service Manager by issuing either, as super user:

```
ps -ef
```

from the OMVS shell, or:

```
d omvs,a=all
```

from the z/OS console. Two processes will be running:

```
WEBSRV 67895616 51118403 - 11:09:59 ttyp0000 0:03 java -Djava.compiler=o
ff -classpath .:sm.zip:ibmjndi.jar:jndi.jar:jsdk.jar:ods
WEBSRV 51118403 84672827 - 11:09:59 ttyp0000 0.00 /bin/sh ./ServiceManag
er.sh
```

You must issue the **kill** command with the PID of the Java -classpath process even though the ServiceManager.sh process is the parent. For example:

```
kill -9 67895616
```

The **ServiceManager.sh** shell script issues the Java command that actually starts the server. If you kill the ServiceManager.sh process, the Java -classpath process remains. Then, if you try to restart the Service Manager, you will receive the following error:

```
remote.Server. : ServerSocket Constructor Failed: EDC8115I Address already
in use.
*** Error - Failed to start Service Manager on port 8999
```

You must kill the Java -classpath process so the ServiceManager.sh process will also be killed, and then the server can be restarted. You can create a shell script to kill Host On-Demand as shown in Example 3-5. In this example, we created a shell script, **stophodsrv.sh**, in the /private directory.

Example 3-5 Shell script to kill Host On-Demand

```
#!/bin/sh
#
HODTMP1=/tmp/tmp1
HODTMP2=/tmp/tmp2
HODTMP3=/tmp/tmp3
#
echo "Shell script looking for HODSRV group process id and kill it"
#
ps -e -o pgid,pid,ppid,args >$HODTMP1
egrep "ServiceManager.sh" $HODTMP1 >$HODTMP2
if test ! $? -eq 0
then
   echo "Could not find the Host On-Demand ServiceManager"
   echo
   exit 1
fi
i=0
while test $i -lt 1
do
  read gprocid cprocid pprocid junk
  echo $gprocid $cprocid $pprocid
  let i=$i+1
done <$HODTMP2 >$HODTMP3
echo "killing HODSRV group process  " $gprocid
kill -- -$gprocid
rm $HODTMP1
rm $HODTMP2
rm $HODTMP3
```

The shell script can also be executed from an MVS procedure. A sample procedure is shown in Example 3-6, **`stophodsrv.sh`** is the name of the script we created in Example 3-5.

Example 3-6 Procedure to kill Host On-Demand

```
//STOPHOD PROC
//*********************************************************************
//STOPHOD   EXEC PGM=BPXBATCH,REGION=0K,TIME=NOLIMIT,
//    PARM='sh /usr/lpp/HOD/hostondemand/private/stophodsrv.sh'
//SYSPRINT DD SYSOUT=T
//SYSIN    DD DUMMY
//SYSERR   DD SYSOUT=T
//STDOUT   DD SYSOUT=T
//STDERR   DD SYSOUT=T
//SYSOUT   DD SYSOUT=T
//***STDENV   DD PATH='/etc/leopt'
```

3.3.8 Considerations when running multiple TCP/IP stacks

If you are running multiple TCP/IP stacks, you may need to establish affinity to a specific stack by setting the `_BPX_SETIBMOPT_TRANSPORT` environment variable. The variable can be set in one of two ways: add the variable to the ServiceManager.sh shell script or create a data set or PDS member that contains the environment variable and is pointed to by the SYSENV DD name in the started task. We recommend having a data set with the environment variable and not editing the ServiceManager.sh shell script. We do not recommend adding the environment variable to the /etc/profile in the event other processes will be establishing affinity to other stacks.

```
export _BPXK_SETIBMOPT_TRANSPORT=xxxxxx
```

where `xxxxxx` is the name of the TCP/IP stack with which you want to establish affinity.

If you have multiple stacks and it is not necessary to establish affinity to a specific stack, then do not set the `_BPXK_SETIBMOPT_TRANSPORT` environment variable. The Host On-Demand server will bind to each stack that is active, and can be accessed by the host name of each stack as long as a Web server is active on each stack.

3.3.9 Miscellaneous information

The following are additional functions that a z/OS user should be concerned with.

O/S400 Proxy Server port

By default the O/S400 Proxy Server is automatically started, and it listens on port 3470. If the O/S400 Proxy Server is not required, it may be disabled by following these instructions:

1. Start the Service Manager and log on to the administration applet from a workstation.
2. Select **OS/400 Proxy Server** in the left frame.
3. Select the **No** radio button, then click **Apply**.
4. Log off the administration applet.
5. Stop and restart the Service Manager and the port 3470 will no longer be open.

For more information on the O/S400 Proxy Server, refer to Chapter 10, “OS/400 Proxy” on page 397.

Web server timeout directives

During the download of the cached client from a z/OS Host On-Demand server, you may encounter what appears to be a hang. The default values of the Web server timeout values may not be sufficient for Host On-Demand clients, especially for dial-up connections. We recommend the following start values for the timeout directives in the httpd.conf file if you are supporting dial-up users:

```
InputTimeout        10 min
OutputTimeout       20 min (may need to be increased for slow connections)
ScriptTimeout       10 min
PersistTimeout      20 sec
```

You may need to adjust the values based on your environment. Refer to *z/OS HTTP Server Planning, Installing and Using,* SC34-4826.

Removing Host On-Demand on z/OS

To remove Host On-Demand on the z/OS platform, you must use SMP/E to delete the product from the SMP/E environment. Refer to the *SMP/E V3R2 for z/OS and OS/390: User's Guide*, SA22-7773, and *SMP/E V3R2 for z/OS and OS/390: Reference*, SA22-7772 to delete the product.

Error starting Service Manager, address already in use

If you receive an error message indicating the port address is already in use when starting the Service Manager, you need to check the IPL parameters in the BPXPRMxx member of SYS1.PARMLIB. In the FILESYSTYPE for the transport type of CINET, the parameters INADDRANYPORT and INADDRANYCOUNT reserve ports that the system will use. If the port you have specified for Host On-Demand is in the range specified by these parameters, Host On-Demand cannot use the port. For details on these parameters, refer to *z/OS V1R4.0 MVS Initialization and Tuning Reference*, SA22-7592. The port can also be reserved through the z/OS Communications Server TCP/IP stack.

3.4 TN3270E contention-resolution function

The Telnet TN3270E protocol (RFC 2355) includes enhancements that support contention-resolution. Contention-resolution supports TN3270E server notification to the TN3270E client when data transmission has completed. However, several bugs persist in its implementation that have not been fixed by the IETF.

HOD 7.0.2 introduced TN3270E client functionality to support contention-resolution. By default, Host On-Demand enables the contention-resolution function on TN3270E clients.

A Telnet server that supports TN3270E is required to take advantage of TN3270E enhancements. All IBM TN3270 servers support the TN3270E extensions. However, correct maintenance must be installed on Communications Server for z/OS V1.2 and higher, or COMM665, or similar hang situations can occur. There are a couple of ways to handle the contention-resolution problem on z/OS:

- Apply the following APARs to Communications Server for z/OS, which will fix the problems in its contention-resolution code:
  - PQ72265
  - PQ72970 (this will allow the coding of NOSNAEXT to take effect)

  Other APARs we suggest to have applied:
  - PQ75437
  - PQ74648

  Info APAR II13135 has more information regarding this and other maintenance for the Telnet server on z/OS.
- You can disable contention-resolution all together either on the Communications Server for z/OS side by coding NOSNAEXT in the TCPIP.PROFILE as discussed below. Or, if you are using the Deployment Wizard, by coding the HTML parameter input in the appropriate fields of the Deployment Wizard's Advanced Options window (see “TN3270E” under “3270/5250 Connection selection” on page 280):
  - Name: NegotiateCResolution
  - Value: false

On Communication Server for z/OS 1.2 and higher, contention-resolution is enabled by default, but can be disabled by coding NOSNAEXT under TELNETPARMS in the TCPIP.PROFILE. However, PQ72970 is required for this to work.

3.5 Deployment Wizard considerations

The Deployment Wizard does not run on z/OS, but runs only on a Windows platform. The Deployment Wizard can be installed on a Windows platform from either a Host On-Demand Windows CD or by downloading setupDW.exe from HODMain.html. For further instructions, see 14.2, “Starting the Deployment Wizard” on page 518.

3.5.1 Deployment Wizard files

The administrator can select the type of output to be generated by the Deployment Wizard. If output HTML is selected a number of files will be generated which must be transferred to the z/OS server. If output zip is checked the Deployment Wizard will create a zip file. After the zip file has been transferred to the z/OS server, it can be unzipped using the DWunzip utility. For detailed information about using the Deployment Wizard, refer to Chapter 14, “Deployment Wizard” on page 517.

All Deployment Wizard output must be transferred to the z/OS server in binary mode, and the names are case-sensitive. We recommend using FTP to transfer the file to the z/OS server.

> **Tip:** We recommend using the DWunzip utility as the tool creates files in the appropriate directory, appends the necessary file extensions, and sets file permissions.

Transferring Deployment Wizard output zip files

For our example of using the Deployment Wizard, we selected the HTML-based model to configure two 3270 sessions. The file name created is called *RaleighITSO*. After checking output zip, RaleighITSO.zip was created by the Deployment Wizard. In this example, the HTML file will be published from a separate user directory: /var/hod/customHTML.

Once a zip file is created, follow these steps to deploy the files to the z/OS system:

1. Start an FTP session with your z/OS server system from the workstation.
2. Use the binary command to ensure the transfer mode is Image.
3. Change directory on the target system to your publish directory. This will either be the Host On-Demand publish directory or your user publish directory. In this scenario we will use our user publish directory:

   ```
   cd /var/hod/customHTML
   ```

4. Change directory on the local client to the directory where the zip file resides. For example:

   ```
   lcd c:\DWizard\ZIPfiles
   ```

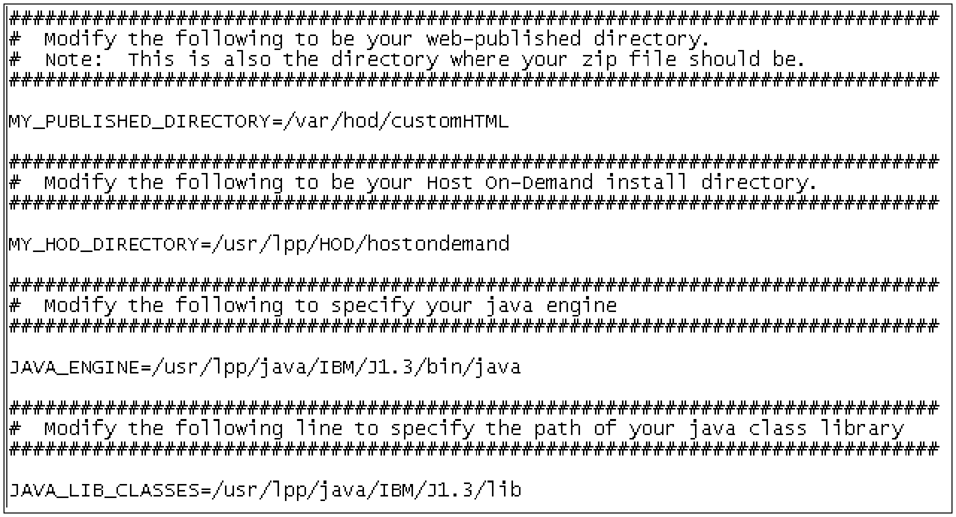
5. Transfer the zip file:

   ```
   put RaleighITSO.zip RaleighITSO.zip
   bye
   ```

6. Log on to your z/OS server and change directory to where the DWunzip file is located. The z/OS DWunzip file is called DWunzip-S390, and located in the Host On-Demand /lib/samples/DWunzipCommandFiles directory. For example:

```
cd /usr/lpp/HOD/hostondemand/lib/sample/DWunzipCommandFiles
```

Edit DWunzip-S390, modifying the parameters to your installation directories as shown in Figure 3-3. If you have created a separate user publish directory, modify MY_PUBLISHED_DIRECTORY to reflect this directory. Verify DWunzip has execute permissions. Use the **chmod** command to set the permissions if required. If you have mounted the Host On-Demand HFS as read-only, you will need to copy DWunzip-S390 to a directory with write permissions in order to update the file with your installation variables.



```
###############################################################################
#  Modify the following to be your web-published directory.
#  Note:  This is also the directory where your zip file should be.
###############################################################################

MY_PUBLISHED_DIRECTORY=/var/hod/customHTML

###############################################################################
#  Modify the following to be your Host On-Demand install directory.
###############################################################################

MY_HOD_DIRECTORY=/usr/lpp/HOD/hostondemand

###############################################################################
#  Modify the following to specify your java engine
###############################################################################

JAVA_ENGINE=/usr/lpp/java/IBM/J1.3/bin/java

###############################################################################
#  Modify the following line to specify the path of your java class library
###############################################################################

JAVA_LIB_CLASSES=/usr/lpp/java/IBM/J1.3/lib
```

Figure 3-3 DWunzip-S390

Transferring Deployment Wizard Output HTML files

If **Output HTML** is selected, you will need to transfer all the Deployment Wizard files in binary to the z/OS server. You will also need to append .ascii to the .html and .txt files.

In this example, using the Deployment Wizard and the HTML-based model we created two 3270 sessions. The file name entered was Raleigh2ITSO and the Output HTML was checked. See Example 3-7 for a list of files that was created by the Deployment Wizard. In this example the HTML file will be published from the Host On-Demand publish directory.

Example 3-7 Sample Output HTML Deployment Wizard files

```
hostondemand\HOD\Raleigh2ITSO.html
hostondemand\HOD\z_Raleigh2ITSO.html
hostondemand\HOD\HODData\Raleigh2ITSO\cfg0.cf
hostondemand\HOD\HODData\Raleigh2ITSO\cfg1.cf
hostondemand\HOD\HODData\Raleigh2ITSO\params.txt
hostondemand\HOD\HODData\Raleigh2ITSO\policy.obj
```

```
hostondemand\HOD\HODData\Raleigh2ITSO\preloads.obj
hostondemand\HOD\HODData\Raleigh2ITSO\udparams.txt
hostondemand\HOD\HODData\Raleigh2ITSO\wInfo.txt
```

Follow the following steps to copy the files to the z/OS server:

1. Start an FTP session with your z/OS server system from the workstation.
2. Use the binary command to make sure the transfer mode is Image.
3. Change directory on the target system to the Host On-Demand publish directory or your user publish directory. In this example we have used the Host On-Demand publish directory:

   ```
   cd /usr/lpp/HOD/hostondemand/HOD
   ```

4. Change directory on the local client to the directory where the files reside. For example:

   ```
   lcd c:\DWizard\HTMLfiles
   ```

5. Transfer the files, renaming the .html and .txt files to append .ascii as shown in Example 3-8.

Example 3-8 FTP Deployment Wizard generated files to z/OS

```
put Raleigh2ITSO.html Raleigh2ITSO.html.ascii
put z_Raleigh2ITSO.html z_Raleigh2ITSO.html.ascii
mkdir HODData
cd HODData
mkdir Raleigh2ITSO
cd Raleigh2ITSO
lcd HODData\Raleigh2ITSO
mput cfg*.*
put params.txt params.txt.ascii
mput p*.obj
put udparams.txt udparams.txt.ascii
put wInfo.txt wInfo.txt.ascii
bye
```

6. Verify the permissions are 755 of all the files, including the subdirectories HODData and Raleigh2ITSO. If they are not, change them using the **chmod** command, either through the FTP session, or by logging on to the z/OS system on TSO.

The customized client is now ready to be downloaded. If the Host On-Demand server and Web server were active before you uploaded, you do not need to recycle them to pick up the new HTML files.

If you are updating an existing customized HTML file, you should stop the Web server prior to uploading, since the FTP may fail if the custom page is in use.

3.6 Using SSL with Communications Server for z/OS

Communications Server for z/OS supports data encryption through the Secure Sockets Layer (SSL) protocol. Beginning with Communications Server for OS/390 V2R10, the use of RACF as a repository for the server's keyring is supported. OS/390 V2R10 also introduced the TELNETPARMS CONNTYPE statement that allows a client to connect to a Telnet port either as secured or basic, which allows security negotiation on a single port.

There are three main scenarios:

- A Host On-Demand client can be configured to make an SSL-secured connection directly to a Communications Server for z/OS server, having been loaded from a separate Host On-Demand server.
- A Host On-Demand Redirector on Windows or AIX can be configured to make an outgoing SSL connection to a Communications Server for z/OS.
- When a Host On-Demand server and Communications Server for z/OS are installed on the same system, a client downloaded from z/OS can make an SSL connection to the z/OS Telnet server without the use of the Redirector.

The z/OS setup required for scenarios 1 and 2 is the same. Communications Server for z/OS uses gskkyman for its key management and the keyring database is of the kdb type. The procedure for putting the server's site certificate into the CustomizedCAs.p12 file is as follows:

1. On the z/OS, create the keyring file and a certificate request using **`gskkyman`**.
2. Store the unknown CA's certificate into the key database.
3. Receive the signed certificate into the key database.
4. Update the CustomizedCAs.p12.

Scenario 3 is different because the key management utility on z/OS is not able to add the certificate to the class file database, CustomizedCAs.p12. However, a Java program named keyrng.class is provided by Host On-Demand to add the certificate to the CustomizedCAs.p12 file. This is demonstrated in "Make certificates available to clients" on page 103.

3.6.1 Telnet Server and SSL support

The z/OS TN3270 Telnet server supports the Secure Sockets Layer (SSL) protocol. This provides secure data transmission between a secure port and an SSL-enabled client. SSL supports three levels of client authentication (allowing additional authentication and access control by means of a certificate that must be presented to the server by a client):

- Client authentication defined in the SSL specification, Level 1
- Client authentication against the certificate stored in RACF, Level 2

- Client authentication with the SERVAUTH RACF class, Level 3

In the TCP/IP profile, three keywords can be used for the CLIENTAUTH parameter in the TELNETPARMS block:

NONE Indicates that no client authentication is required during the SSL handshake

SSLCERT Specifies that the SSL handshake process authenticates the client certificate as well as the server certificate. This is Level 1 security support.

SAFCERT Indicates the additional validation associated with Levels 2 and 3. Level 2 requires the certificate to be stored in RACF, and Level 3 requires the SERVAUTH RACF class is in effect.

In Communications Server for OS/390 V2R10, the Security Server (RACF) provided common keyring support, so no key database is required. All certificates can be managed through the RACF database.

Telnet-negotiated session

A Telnet-negotiated session determines if the security negotiations between the client and the Telnet server are done on the established Telnet connection or on an SSL connection prior to the Telnet negotiation. For the client to use this feature, the Telnet server must support Telnet-negotiated security. The other SSL options are valid regardless of whether Telnet-negotiated is set to `Yes` or `No`.

In OS/390 V2R10 or above, the `CONNTYPE ANY` keyword in the TELNETPARMS block signifies that the Telnet server can support both SSL clients and non-SSL clients over a single port. The Telnet server first establishes a Telnet session then negotiates security. If the client wishes to enter into a secure connection, SSL protocols will be used for all subsequent communication. If the client is not willing to enter a secure connection, a non-SSL or basic connection is used. For a complete discussion of Telnet-negotiated sessions, refer to “Telnet-negotiated sessions” on page 1043.

Note: Do not use `CONNTYPE ANY` if you are going through a firewall, because this will allow a non-SSL connection through the firewall. For details about the `CONNTYPE` keyword, refer to the *IBM Communications Server IP Configuration Reference* manual for your operating system release.

3.6.2 SSL encryption overview

Host On-Demand V8 has one FMID providing all the encryption support: HHOJ800.

In an SSL-encrypted session, any data on a secure port is encrypted by means of the SSL protocol before it is sent to the client. Data received from the client is decrypted before the data is sent to other processes, such as VTAM®. The flows between Telnet and VTAM are unchanged.

Secure connections are made through a secure port. When running with base TCP/IP, Telnet connections across ports defined as secure are protected by way of MD5 or SHA hashing algorithms and support SSL V3 clients, but do not provide data encryption. SSL Encryption support by way of RC2, RC4, DES, or triple DES requires one of the optional features shown in the tables below.

The following table describes the FMIDs for the respective levels of OS/390 and z/OS.

Table 3-1 Encryption FMIDs

Encryption Feature	Base	Level 1	Level 2	Level 3
V2R10	HTCP50A	HTCP53A	HTCP52A	JTCP5KA
zOS V1R1	HTCP50A	HTCP53A	HTCP52A	JTCP5KA
zOS V1R2	HIP6120	N/A	N/A	JIP612K
zOS V1R3	HIP6120	N/A	N/A	JIP612K
zOS V1R4	HIP6140			JIP614K

The following table provides the level of security that each level provides.

Table 3-2 Encryption features for OS/390

Level	SSL V3 Clients	SSL V2 Clients
Base	NULL SHA NULL MD5 NULL NULL	Not supported
Level 1	RC4 MD5 Export RC2 MD5 Export NULL SHA NULL MD5 NULL NULL	RC4 Export RC2 Export
Level 2	DES SHA RC4 MD5 Export RC2 MD5 Export NULL SHA NULL MD5 NULL NULL	RC4 Export RC2 Export

Level	SSL V3 Clients	SSL V2 Clients
Level 3	Triple DES SHA US DES SHA RC4 MD5 Export RC4 SHA US RC4 MD5 US RC2 MD5 Export NULL SHA NULL MD5 NULL NULL	Triple DES US DES US RC4 Export RC4 US RC2 Export RC2 US

Refer to “Basic concepts of cryptography and digital certificates” on page 1010 for descriptions of the encryption elements.

For more information about the security levels, please refer to:

- *z/OS Communications Server: IP Configuration Reference,* SC31-8776

You can find additional information on the following Web sites:

- About SSL protocol:

  `http://home.netscape.com/eng/ssl3/ssl-toc.html`

- About the encryption methodology:

  `http://www.verisign.com/repository/crptintr.html`

3.6.3 SSL configuration using gskkyman

In this section, we discuss the use of the **gskkyman** utility to do the following:

- Create the key database
- List all trusted CAs
- Create key pair and certificate request
- Store a CA certificate
- Receive a certificate issued for the request
- Create a self-signed certificate
- Make certificates available to clients
- Implement Server Authentication using a certificate from an unknown Certificate Authority
- Implement Client authentication
- Transport Layer Security-based security (OS/390 V2R10 and higher)

Create the key database

If you do not have a key database, you must create it using either the **gskkyman** utility, which is shipped as part of the Cryptographic Services, or the Security Server (RACF) if on OS/390 V2R10 or higher.

> **Note:** When using **gskkyman**, do not create your key database in any of the Host On-Demand directories for security and migration reasons.

If using **gskkyman**, go to the OMVS shell and follow the steps shown in Example 3-9. Before using the utility, you might need to make **gskkyman** known to the UNIX System Services environment:

`export STEPLIB=GSK.SGSKLOAD` (verify name)

Example 3-9 Creating the key database

```
CASEY @ SC48:/u/casey>gskkyman


            IBM Key Management Utility

Choose one of the following options to proceed.

   1  - Create new key database
   2  - Open key database
   3  - Change database password

   0  - Exit program

Enter your option number: 1
Enter key database name or press ENTER for "key.kdb": itso.kdb
Enter password for the key database.......>
Enter password again for verification.....>
Should the password expire? (1 = yes, 0 = no) 1¨: 0

The database has been successfully created, do you want to continue to work
with the database now? (1 = yes, 0 = no) 1¨: 1


            Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 11

The encrypted password has been stored in file /u/casey/itso.sth

Your request has completed successfully, exit gskkyman? (1 = yes, 0 = no) 0¨: 0
```

After creating the key database, you need to store the encrypted database password, option 11. This creates a .sth stash file.

List all trusted CAs

Next, we need to determine if the Certificate Authority you plan to use is in the list of trusted CAs (Example 3-10). If you plan to use a self-signed certificate, refer to “Create a self-signed certificate” on page 101.

Example 3-10 List trusted Certificate Authorities this key database knows

```
             Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 10


            Trust CA certificate list

Key database name is /u/casey/itso.kdb
```

```
Please choose one of the following keys to work with.

    1  - Integrion Certification Authority Root
    2  - IBM World Registry Certification Authority
    3  - Thawte Personal Premium CA
    4  - Thawte Personal Freemail CA
    5  - Thawte Personal Basic CA
    6  - Thawte Premium Server CA
    7  - Thawte Server CA
    8  - Verisign Test CA Root Certificate
    9  - RSA Secure Server Certification Authority

Enter a key number or press ENTER for more labels:  <Enter>
            Trust CA certificate list

Key database name is /u/casey/itso.kdb

Please choose one of the following keys to work with.

    10  - Verisign Class 1 Public Primary Certification Authority
    11  - Verisign Class 2 Public Primary Certification Authority
    12  - Verisign Class 3 Public Primary Certification Authority

Enter a key number or press ENTER to return to parent menu: <Enter>
```

Create key pair and certificate request

If you need to request a certificate to be signed by a well-known Certificate Authority or an unknown Certificate Authority, you need to create a key pair and certificate request (Example 3-11).

Example 3-11 Create new key pair and certificate request

```
             Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password
```

```
     0  - Exit program


Enter option number (or press ENTER to return to the parent menu): 3
Enter certificate request file name or press ENTER for "certreq.arm":
itsoreq.arm
Enter a label for this key................> ITSO Certificate
Select desired key size from the following options (512):
    1:    512
    2:    1024
Enter the number corresponding to the key size you want: 2
Enter certificate subject name fields in the following.
    Common Name (required)................> wtsc48oe.itso.ibm.com
    Organization (required)...............> IBM
    Organization Unit (optional)..........> ITSO
    City/Locality (optional)..............> RTP
    State/Province (optional).............> NC
    Country Name (required 2 characters)..> US

Please wait while key pair is created...

Your request has completed successfully, exit gskkyman? (1 = yes, 0 = no) 0¨: 1
```

The label you enter will be the label you see when you display the list of certificates.

The common name is the fully qualified host name of the TN3270 server. If you select **server authentication** on the Host On-Demand session properties, the common name must match the host name in the DNS server for the IP address of the TN3270 server. In our example, the host name of our TN3270 server is `wtsc48oe.itso.ibm.com`.

Using the file that was created (in our example, `itsoreq.arm`) you can then send the request to the Certificate Authority of your choice. For these examples, we set up an ITSO Certificate Authority server for signing certificates.

Store a CA certificate

After you receive the signed certificate from the CA, you need to add the unknown CA certificate to your list of Trusted CAs (Example 3-12). Enter **`gskkyman`** and open the key database you previously created. If you requested a certificate from a CA already in the trusted list, you can skip this step and go to “Receive a certificate issued for the request” on page 100.

Example 3-12 Store a CA certificate

```
            Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 6
Enter certificate file name or press ENTER for "cert.arm": itsoca.cer
Enter a label for this key................> ITSO Certificate Authority

Please wait while certificate is stored...

Your request has completed successfully, exit gskkyman? (1 = yes, 0 = no) 0¨: 0

            Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 10

            Trust CA certificate list
```

```
Key database name is /u/casey/itso.kdb

Please choose one of the following keys to work with.

    1  - ITSO Certificate Authority
    2  - Integrion Certification Authority Root
    3  - IBM World Registry Certification Authority
    4  - Thawte Personal Premium CA
    5  - Thawte Personal Freemail CA
    6  - Thawte Personal Basic CA
    7  - Thawte Premium Server CA
    8  - Thawte Server CA
    9  - Verisign Test CA Root Certificate

Enter a key number or press ENTER for more labels: 1

                   Key Menu

Currently selected key: ITSO Certificate Authority

Choose one of the following options to proceed.

    1  - Show key information
    2  - Set the selected key as default
    3  - View certificate of the key
    4  - Remove trust root status
    5  - Copy the certificate of this key to a file
    6  - Delete the key
    7  - Export the key to another database

    0  - Exit program

Enter option number (or press ENTER to return to the parent menu):1


     Basic information of the currently selected key

                     Unique ID:    13
                         Label:    ITSO Certificate Authority
         Chosen as default key:    false
                      Key size:    1024
                Set as trusted:    true
         Private key existence:    false
  User defined field existence:    false


     Certificate information for the selected key
```

```
                Version:    3
          Serial number:    0582cf5027da20a945f0dadf594849b1
            Issuer name:
                            ITSORaleigh
                            ITSO
                            IBM
                            Raleigh, NC
                            US
                            mticknor@us.ibm.com
           Subject name:
                            ITSORaleigh
                            ITSO
                            IBM
                            Raleigh, NC
                            US
                            mticknor@us.ibm.com
         Effective date:    08/27/02
        Expiration date:    08/27/04
Signature algorithm OID:    sha1WithRSASignature
       Issuer unique ID:    false
      Subject unique ID:    false
   Number of extensions:    5
```

Choosing to list all trusted CAs shows the new CA as trusted, and then you can show the key information. You cannot make this certificate the default at this time. Once a private key from this CA has been added to the key database, then the certificate can be made the default.

Receive a certificate issued for the request

Once you receive the signed certificate from the CA, you can receive the certificate into the key database for your request (Example 3-13).

Example 3-13 Receive certificate after signed by CA

```
            Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
```

```
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 4
Enter certificate file name or press ENTER for "cert.arm": itso.cer
Do you want to set the key as the default in your key database? (1 = yes, 0 =
no) 1¨: 1

Please wait while certificate is received......

Your request has completed successfully, exit gskkyman? (1 = yes, 0 = no) 0¨:1
```

Create a self-signed certificate

Using **gskkyman**, you can create a self-signed certificate (Example 3-14). Once the certificate is created, make this certificate the default.

Example 3-14 Creating a self-signed certificate

```
Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 5
Enter version number of the certificate to be created (1, 2, or 3) Ý3¨:  3
Enter a label for this key................> ITSO self-signed cert
Select desired key size from the following options (512):
    1:    512
    2:    1024
Enter the number corresponding to the key size you want: 2
Enter certificate subject name fields in the following.
    Common Name (required)...............> wtsc48oe.itso.ibm.com
    Organization (required)..............> IBM
    Organization Unit (optional).........> ITSO
    City/Locality (optional).............> RTP
    State/Province (optional)............> NC
    Country Name (required 2 characters)..> US
Enter number of valid days for the certificate Ý365¨:  365
Do you want to set the key as the default in your key database? (1 = yes, 0 =
no) Ý1¨: 1
Do you want to save the certificate to a file? (1 = yes, 0 = no) Ý1¨: 1
Should the certificate binary data or Base64 encoded ASCII data be saved? (1 =
ASCII, 2 = binary) 1¨: 2
Enter certificate file name or press ENTER for "cert.crt": itsoself.crt

Please wait while self-signed certificate is created...

Your request has completed successfully, exit gskkyman? (1 = yes, 0 = no) 0¨: 0

            Key database menu

Current key database is /u/casey/itso.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 10

            Trust CA certificate list

Key database name is /u/casey/itso.kdb

Please choose one of the following keys to work with.

    1  - ITSO self-signed cert
    2  - ITSO Site Certificate
    3  - ITSO Certificate Authority
    4  - Integrion Certification Authority Root
    5  - IBM World Registry Certification Authority
    6  - Thawte Personal Premium CA
```

```
   7  - Thawte Personal Freemail CA
   8  - Thawte Personal Basic CA
   9  - Thawte Premium Server CA

Enter a key number or press ENTER for more labels:
```

The label you enter will be the label you see when you display the list of certificates.

The common name is the fully qualified host name of the TN3270 server. If you select **server authentication** on the Host On-Demand session properties, the common name must match the host name in the DDNS server for the IP address of the TN3270 server.

Make certificates available to clients

The process of making the server's public certificate available varies with the type of client. The locally installed client obtains the server certificate from the same sources as the download and cached clients, the CustomizedCAs.p12 file or the Microsoft cryptographic database. However, on a locally installed client the CustomizedCAs.p12 file must reside on the client itself. There are two methods of updating this file on the client. We recommend the first method:

- Have the administrator create the CustomizedCAs.p12 file for the download clients, then distribute it to every locally installed user.
- Distribute the certificate to every locally installed user and have them run the Certificate Management Utility to create or update their local copy of the CustomizedCAs.p12 file. The procedure for doing this is the same as described in "Creating the CustomizedCAs.p12 file on the server" on page 104.

Downloaded and cached clients must be able to access the certificate from the Host On-Demand server. If the server is using a certificate from a well-known trusted CA, nothing more needs to be done because the certificate is already in the WellKnownTrustedCAs.class file in the publish directory. Therefore, it is accessible to the clients.

The Telnet server's certificate issued from an unknown CA, or a self-signed certificate, can be made available to the client in one of two ways:

- If the client is running on a Windows platform, you add the certificate to the MSIE browser's keyring. This action is not automatic and must be performed by each user. Refer to 11.4.5, "Add MSIE browser's keyring" on page 429 for the procedures on how to do this.
- Create a CustomizedCAs.p12 file, store it on the server, and it will be downloaded to the client.

Creating the CustomizedCAs.p12 file on the server

If the certificate is self-signed or from an unknown Certificate Authority, you should put it into the CustomizedCAs.p12 file in the publish directory using the Java keyring utility. The publish directory can be either the Host On-Demand server publish directory or a separate user directory. See *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301. The utility can be issued one of two ways, either with the add option or connect option. We recommend the connect option because it issues a socket connection to the TCP/IP SSL port, and verifies it is available and configured correctly.

Before you can issue the Java keyring utility, you need to have the TCP/IP TN3270 Telnet server configured for the SSL port you wish to connect. For TCP/IP profile definitions see “Configuring TCP/IP TN3270 server for SSL” on page 108. Run the Java keyring utility provided with Host On-Demand. This is a lengthy command and it is easy to make errors. The backslash is a continuation character; otherwise, the command must be on one continuous line. The command for Java 1.3 is:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs connect ipaddr:port
```

where `ipaddr` is the address of your TN3270 Telnet server and `port` is the SSL port you wish to connect.

> **Tip:** You can create a shell script with the command. This enables you to easily reissue the command if needed. It also allows you to check the syntax of the command before running the script.

You will be prompted to enter the password for the CustomizedCAs.p12 file. You *must* give a password. The password must be **hod** (all lower case letters), or it will not work. The results of the command will look similar to the Java 1.3 example shown in Example 3-15.

Example 3-15 Java keyring utility output

```
CASEY @ SC48:/usr/lpp/HOD/hostondemand/HOD>javakeyrng
Password for CustomizedCAs.p12:
Connecting to 9.12.6.126:6623
com.ibm.hodsslight.SSLException
       at com.ibm.hodsslight.SSLConnection.certificate(SSLConnection.java:979)
       at com.ibm.hodsslight.SSLClient.serverCertificate(SSLClient.java:272)
       at com.ibm.hodsslight.SSLClient.handshake(SSLClient.java:110)
        at
com.ibm.hodsslight.SSLConnection.handleData(SSLConnection.java(Compiled Code))
        at
com.ibm.hodsslight.SSLRecordLayer.receiveRecord(SSLRecordLayer.java:695)
       at com.ibm.hodsslight.SSLConnection.install(SSLConnection.java:212)
```

```
        at com.ibm.hodsslight.SSLClient.<init>(SSLClient.java:719)
        at com.ibm.hodsslight.SSLSocket.install(SSLSocket.java:117)
        at com.ibm.hodsslight.SSLSocket.<init>(SSLSocket.java:260)
        at com.ibm.hodsslight.tools.keyrng.main(keyrng.java)
com.ibm.hodsslight.SSLException
 time created=Wed Aug 29 16:52:27 EDT 2002
 category=4  TRUSTPOLICY
 error=1017  PEERCERTIFICATECHAINNOTTRUSTED
 int1 =0
 e=null

-------------------------- Server Certificate Chain --------------------------

Site Certificate - Number 0

        Key : RSA/512 bits
     Subject: wtsc48oe.itso.ibm.com, Research Triangle Park, ITSO, IBM, US
      Issuer: ITSORaleigh, Raleigh, ITSO, IBM, US
  Valid from: Mon Aug 27 10:53:17 EDT 2002
    Valid to: Tue Aug 27 11:03:17 EDT 2003
Finger print: 2A:84:BA:46:C0:73:7C:4F:6D:98:AD:B1:44:72:BA:F8

------------------------------------------------------------------------------

Enter the number of the certificate to be added to CustomizedCAs.p12 (q to
quit): 0
Adding the Site Certificate - 0 to CustomizedCAs.p12
Done.
```

The Java exception shown in Example 3-15 can be ignored. You can verify the certificate was added to the CustomizedCAs.p12 file with the following command:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs verify
```

The add option does not require the TN3270 server to be available, since no socket call is issued. You must specify the name of the certificate file as one of the input parameters. The command when using Java 1.3 is:

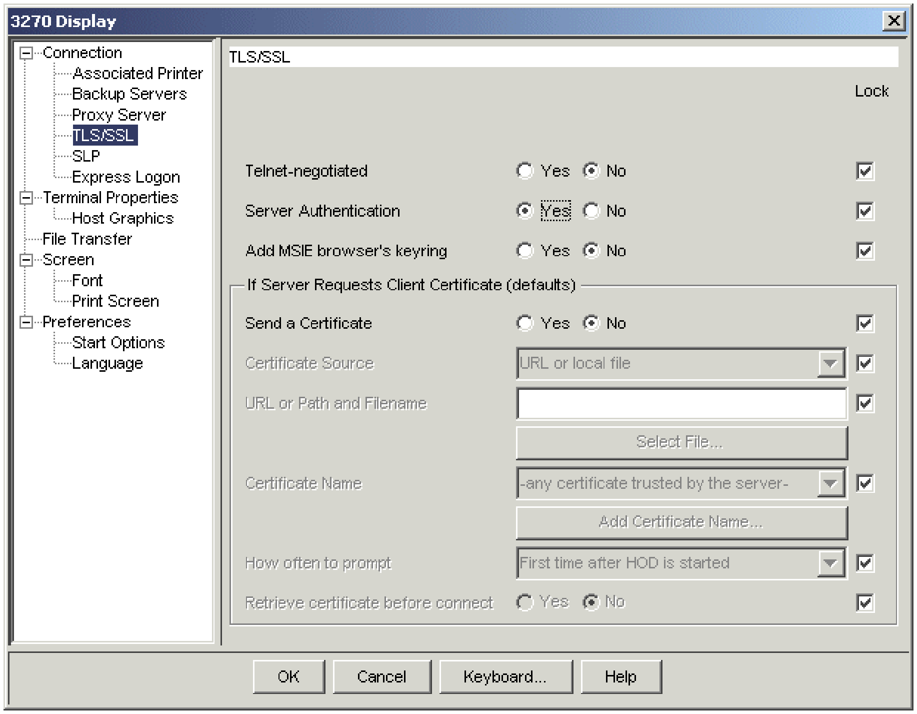
```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs \
add --certificatetype certificate.name
```

Where the certificate type is either `ca` if you are adding a CA root certificate or `site` if you are adding a site or self-signed certificate. The certificate.name is the fully qualified name of the actual certificate, for instance, /u/casey/itso.cer.

Server authentication

For basic SSL TN3270 server authentication connection, you need to configure a port capable of SSL. Refer to “Configuring TCP/IP TN3270 server for SSL” on page 108 for how to define the `TELNETPARMS` definitions.

With the instructions provided for creating a key database, and requesting and receiving a certificate, you should be able to establish a TN3270 SSL connection for server authentication. In the session properties, select **Telnet -TLS** or **Telnet -SSL only** as the protocol and select **Yes** for Server Authentication (SSL) as shown in Figure 3-4.



TLS/SSL

Lock

Telnet-negotiated ○ Yes ● No ☑

Server Authentication ● Yes ○ No ☑

Add MSIE browser's keyring ○ Yes ● No ☑

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No ☑

Certificate Source: URL or local file ☑

URL or Path and Filename ☑

Select File...

Certificate Name: -any certificate trusted by the server- ☑

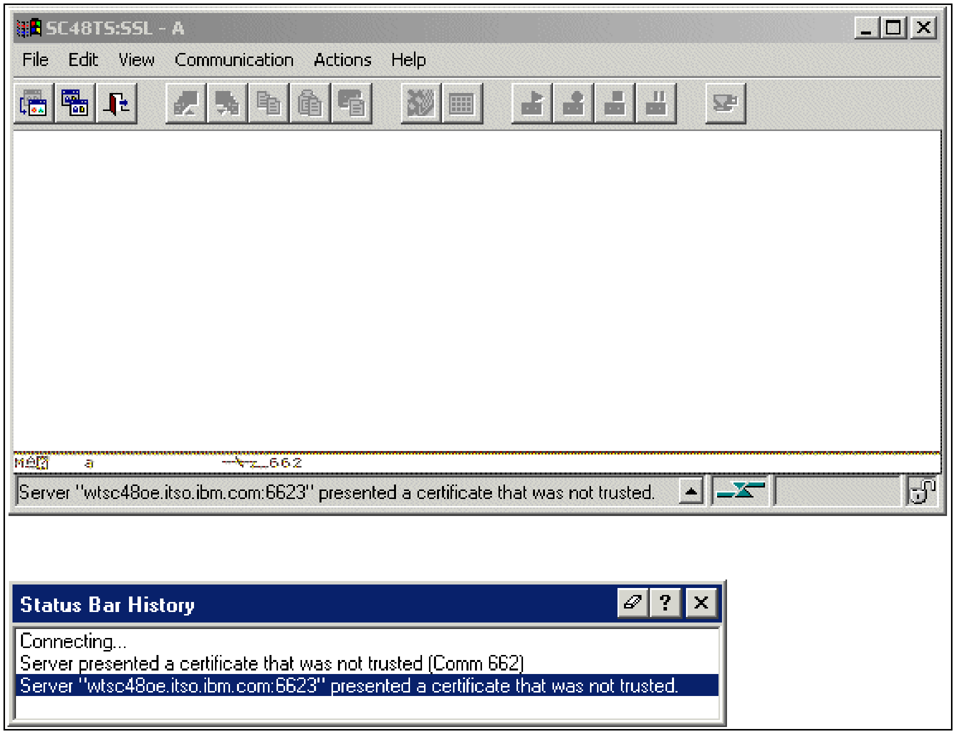
Add Certificate Name...

How often to prompt: First time after HOD is started ☑

Retrieve certificate before connect ○ Yes ● No ☑

Figure 3-4 Session properties to enable SSL for server authentication

When you start the 3270 session the lock in the bottom right corner of the session window should be locked. If it is not, check the communication code on the bottom of the window. Click the up arrow next to the message in the OIA to display the Status Bar History. Click **?** for further details of the error.



Server "wtsc48oe.itso.ibm.com:6623" presented a certificate that was not trusted.

Connecting...
Server presented a certificate that was not trusted (Comm 662)
Server "wtsc48oe.itso.ibm.com:6623" presented a certificate that was not trusted.

Figure 3-5 3270 session fails to connect, communications error

For this example, the CustomizedCAs.p12 file did not exist. It was created using the instructions in “Creating the CustomizedCAs.p12 file on the server” on page 104. In order to download the CustomizedCAs.p12 file, if using Internet Explorer, press and hold Ctrl, then click **Refresh** on the browser to reload the file; if using Netscape, click **Reload**.

Client authentication

In client authentication the Telnet server requests a certificate from the client to verify who it claims to be. To enable client authentication, server authentication must first be enabled. On the Host On-Demand session properties, several options are available to deploy client authentication. Refer to 11.3.3, “Client authentication” on page 423.

Restriction: Host On-Demand requires a Version 3 type certificate for client authentication. If you have created the certificate using GSKKYMAN on z/OS, you will need to convert the Version 1 PKCS12 created on the z/OS to a Version 3 PKCS12 file. The following lists the steps required to convert a PKCS12 Version 1 file to Version 3.

Here are the steps:

1. On the TN3270 server, use GSKKYMAN to create a self-signed certificate.
2. Create a PKCS12 format file (select **Export keys**, **Export keys to a PKCS12 file** from the GSKKYMAN panels). This will create a file with the format filename.p12. If using CLIENTAUTH SAFCERT, use this file as the client certificate source if manually registering the client certificate to the SAF product.
3. FTP the PKCS12 file in binary mode to the client.
4. Use the Host On-Demand certificate management panels to import the PKCS12 file into the Host On-Demand key database.
5. Export the certificate using the Host On-Demand certificate management panels to create a new PKCS12 file. This is the file that Host On-Demand will use to retrieve the client certificate.

On the z/OS TN3270 server, the TCP/IP profile must be configured for client authentication. See below for details on configuring the profile.

Configuring TCP/IP TN3270 server for SSL

To configure client authentication in IP services, the TCP/IP profile must be updated. Configure the TCP/IP profile data set, using the `CLIENTAUTH` statement in the TELNETPARMS block, and choosing the security level you want. Client authentication is only supported by OS/390 V2R8 and higher. Our TCP/IP profile Telnet statements are shown in Example 3-16.

Example 3-16 TCP/IP profile Telnet statements

```
; Basic TN3270 Telnet - non-SSL
TELNETPARMS
  PORT 623
ENDTELNETPARMS

; Basic SSL - provides Server Authentication
TELNETPARMS
  SECUREPORT 6623 KEYRING HFS /u/casey/itso.kdb
  CLIENTAUTH NONE
ENDTELNETPARMS

; Client Authentication, without RACF security
TELNETPARMS
  SECUREPORT 7723 KEYRING HFS /u/casey/itso.kdb
  CLIENTAUTH SSLCERT
ENDTELNETPARMS

; Client Authentication, with RACF security
TELNETPARMS
```

```
  SECUREPORT 8823 KEYRING HFS /u/casey/itso.kdb
  CLIENTAUTH SAFCERT
ENDTELNETPARMS

; Client Authentication, with RACF security and SERVAUTH class active
TELNETPARMS
  SECUREPORT 9923 KEYRING HFS /u/casey/itso.kdb
  CLIENTAUTH SAFCERT
ENDTELNETPARMS

BEGINVTAM
  PORT 623 6623 7723 8823 9923

DEFAULTLUS
    TCP48001..TCP48099
ENDDEFAULTLUS

DEFAULTAPPL SC48TS      ; TSO
  LINEMODEAPPL SC48TS
  ALLOWAPPL *

ENDVTAM
```

The Telnet server configuration can be updated dynamically by using the following command:

```
vary tcpip,,obeyfile,dataset.name
```

3.6.4 Certificate management using RACF

RACF can be used to create, register, store, and administer digital certificates, and the private keys associated with the certificates. RACF can also be used to create and manage keyrings of stored digital certificates. In this section we describe how to manage your certificates using the RACF commands. Certificates are stored in the RACF database, while private keys may be stored in the ICSF Public Key Data Set (PKDS), encrypted under a 168-bit Triple-DES key.

Using RACF keyrings is the preferred method, because it provides better security for the certificates and their private keys. With RACF keyrings, stash files containing key database passwords are not used, and access to keyrings and certificates is controlled by RACF.

RACF distinguishes three types of digital certificates:

- Certificate Authority certificates: These certificates are associated with Certificate Authorities (CAs) and are used to verify signatures in other certificates.
- Site certificates: These certificates are associated with servers or network entities in other locations than the local system.
- User certificates: These certificates are associated with a RACF user ID and are used to authenticate a user's identity.

A user certificate or a certificate that has been connected to a keyring with USAGE(PERSONAL) is the only type of certificate whose private key can be used to create signatures. Therefore, all server certificates for local servers need to be user certificates, or they need to be connected to an appropriate keyring with USAGE(PERSONAL).

The step-by-step example described in "Using a CA-signed certificate" on page 110 is generic in nature. It can be used to create a RACF keyring for the IBM HTTP Server for z/OS, the TN3270 server, or other servers that are SSL enabled.

For detailed information about the RACDCERT command, refer to the *z/OS V1R4.0 Security Server RACF Command Language Reference*, SA22-7687.

Using a CA-signed certificate

This section presents the steps required to implement the SSL environment for the Host On-Demand Server. A similar procedure can be used for other SSL-enabled application servers. In this scenario, we use a server certificate signed by a public CA. The steps are:

1. Generate a self-signed certificate.
2. Create a certificate request for the CA.
3. Store the returned certificate into a data set.
4. Store CA certificate for unknown Certificate Authority.
5. Replace the self-signed certificate.
6. Create a keyring for the server.
7. Connect the certificate to the keyring.
8. Connect the CA certificate to the keyring.

Generate a self-signed certificate

We used this self-signed certificate as a base for the certificate request we created:

```
RACDCERT   ID(STC)   GENCERT
SUBJECTSDN(CN('wtsc48oe.itso.ibm.com')
   O('IBM')
```

```
      OU('ITSO')
      L('RTP')
      SP('NC')
      C('US'))
   WITHLABEL('HOD Server Certificate')
```

Make sure the common name (CN) is the same as the host or domain name of the server. STC is the user ID associated with the TCPIP started task.

Create a certificate request for the CA

The certificate request will be stored in an MVS data set with a name like `'CASEY.HODSRV.GENREQ'`.

```
RACDCERT   ID(STC)   GENCERT
GENREQ(LABEL('HOD Server Certificate'))
DSN('CASEY.HODSRV.GENREQ')
```

This certificate request needs to be sent to the Certificate Authority. The format of the request is Base64-encoded text. The data set can be transmitted to a PC with FTP, and pasted into the appropriate field in the certificate request. Alternatively, cutting and pasting between a host emulator window and the Web browser can be used.

Store the returned certificate into a data set

The CA usually returns the certificate using e-mail or similar means. The certificate is in Base64-encoded text format. Again, use the same technique as before to copy the certificate into a data set named, for instance, `'CASEY.HODSRV.CERT'`.

Note: The data set organization must be variable blocked. If it is fixed blocked, you will receive error IRRD103I: `An error was encountered processing the specified input data set`. You may need to preallocate the data set as variable blocked prior to transferring the signed certificate.

Store CA certificate for unknown Certificate Authority

If your certificate is signed by an unknown Certificate Authority, you need to store the CAs certificate into the RACF database. We created our own Certificate Authority to sign the certificates; therefore, the CA certificate needs to be stored in the RACF database:

```
RACDCERT CERTAUTH ADD('CASEY.HODSRV.CACERT') TRUST
WITHLABEL('HOD Certificate Authority')
```

Replace the self-signed certificate

Replace the self-signed certificate with the certificate received from and signed by the CA:

```
RACDCERT   ID(STC) ADD('CASEY.HODSRV.CERT') TRUST
WITHLABEL('HOD Server Certificate')
```

Create a keyring for the server

This keyring must not already exist for this user. Keyring names becomes names of RACF profiles in the DIGTRING class, and can contain only characters that are allowed in RACF profile names. Although asterisks are allowed in keyring names, a single asterisk is not allowed:

```
RACDCERT ADDRING(HODSERVER)
```

Connect the certificate to the keyring

Now we can create the connection between the digital certificate and the keyring with the RACDCERT CONNECT command, and associate it with the Host On-Demand started task user ID:

```
RACDCERT CONNECT(ID(STC) LABEL('HOD Server Certificate') RING(HODSERVER)
DEFAULT USAGE(PERSONAL))
```

Connect the CA certificate to the keyring,

If you had your certificate signed by an unknown Certificate Authority and have to store the CA certificate in the RACF data base, you need to connect the CA certificate to the keyring:

```
RACDCERT CONNECT(CERTAUTH LABEL('HOD Certificate Authority')
RING(HODSERVER) USAGE(CERTAUTH))
```

3.7 Certificate Express Logon

In previous releases of Host On-Demand and z/OS, Certificate Express Logon was known as the Express Logon Feature (ELF). In Host On-Demand V8, the Express Logon feature was renamed to Certificate Express Logon.

Certificate Express Logon was introduced in IBM Communications Server for OS/390 V2R10 IP Services. Certificate Express Logon allows a user on a workstation (with a TN3270 client and an X.509 certificate) to log on to an SNA application without entering a user ID or password.

Certificate Express Logon allows users to:

- Reduce the time administrators spend maintaining user IDs and passwords.
- Reduce the number of user IDs and passwords that users must remember.

- Remove a potential security risk of users writing down user IDs and passwords, or sharing them with someone else.

For a complete discussion of Certificate Express Logon, refer to 15.2, “Certificate Express Logon” on page 580.

Implementation of two-tier network design

The Certificate Express Logon two-tier design implementation is simpler than the three-tier design implementation, as you no longer need a Digital Certificate Access Server (DCAS) for a middle-tier TN3270 server. Choose the three-tier design if you do not want to have a TN3270 server on z/OS, or if you are going to use Host Publisher. Host Publisher acts as the client and the middle-tier server together.

Follow the steps to implement Certificate Express Logon with the two-tier design, using Host On-Demand as the client and accessing TSO on z/OS:

1. Define an SSL session with client authentication level 2 (CLIENTAUTH SAFCERT in TCP/IP profile). The procedure to define an SSL session is in “Configuring TCP/IP TN3270 server for SSL” on page 108.
2. Define the EXPRESSLOGON parameter on TCP/IP profile. The ITSO profile statements used for Certificate Express Logon are shown in Example 3-17.

Example 3-17 Profile definition for Certificate Express Logon

```
TELNETPARMS
  SECUREPORT 23003
  KEYRING SAF tcpipa.tn3270.keyring
  CONNTYPE SECURE
  CLIENTAUTH SAFCERT
  EXPRESSLOGON
  DEBUG DETAIL
ENDTELNETPARMS
```

3. Define the PassTicket profile to RACF. For each application to which users are to gain access with a PassTicket, you must define a PTKTDATA class profile. In our example, the application is TSO, and the commands issued are those shown in Example 3-18.

Example 3-18 RACF definition for PassTicket

```
SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA)
RDEFINE PTKTDATA TSOSC64 SSIGNON(KEYMASKED(E6C9D30195D4C1E7)) UACC(NONE)
SETR RACLIST(PTKTDATA) REFRESH
```

The profile name (TSOSC64 in our case) must match the application ID configured on the Host On-Demand client window. For TSO, the rule to create a profile name is: TSO+smfid.

Define a key using KEYMASKED, even though the value is not significant. This is required.

For more details about PTKTDATA and rules of profile names, see the *z/OS V1R4.0 Security Server RACF Security Administrator's Guide,* SA22-7683.

4. Next, start TCP/IP and establish a session with port 23002. Now you are ready to create the Certificate Express Logon macro.

You can display the connection to check that Certificate Express Logon is being used as shown in Example 3-19 and Example 3-20.

Example 3-19 Connection display

```
D TCPIP,TCPIPA,T,CONN
EZZ6064I TELNET CONNECTION DISPLAY 664
         EN                                         TSP
CONN     TY IPADDR..PORT           LUNAME   APPLID   PTR LOGMODE
-------- -- --------------------- -------- --------  --- --------
00000F76 4S 9.24.106.91..1347      TCP64002 SC64TS05  TAE D4C32XX3
----- PORT:   23003    ACTIVE          PROF: CURR CONNS:      1
------------------------------------------------------------
3 OF 3 RECORDS DISPLAYED
```

Example 3-20 Connection display details

```
D TCPIP,TCPIPA,T,CONN,CO=F76
EZZ6065I TELNET CONNECTION DISPLAY 689
  CONN: 00000F76           CLNTIP..PORT: 9.24.106.91..1347
  LINKNAME: OSA22E0LINK      DESTIP..PORT: 9.12.6.60..23003
  HOSTNAME: NO HOSTNAME
  CONNECTED: 15:43:14  09/28/2001  STATUS: SESSION ACTIVE
  PORT: 23003 ACTIVE  SECURE       ACCESS: SECURE  4S    SAFCERT  1
  PROTOCOL: TN3270E  LOGMODE: D4C32XX3 DEVICETYPE: IBM-3278-3-E
    OPTIONS: ETET---   3270E FUNCTIONS: BSR----
                      NEWENV FUNCTIONS: E-
  USERIDS
    RESTRICTAPPL: **N/A**   CLIENTAUTH: FASCINI   2
    EXPRESSLOGON: FASCINI  3
  APPL: SC64TS05
  LUNAME: TCP64002  TYPE: TERMINAL GENERIC
  MAPS CONN IDENTIFIER      OBJECT   DEFAPPL          OPTIONS
    LU MAPPINGS:
                           >*DEFLUS* **N/A**          -----
    DEFAULTAPPL:
       NL (NULL)          TSO                        -----
    USS TABLE: **N/A**
    INT TABLE: **N/A**
    PARMS:
  PERS  FUNCT    DIA  SECURE   TIMERS  SMF   MAX  LINE
 (LMTQ)(OATSSWH)(DRF)(SCKLECX)(IKPSTS)(ITIT)(RSQ)(BDCTT)
  ----  -------  ---  -------  ------  ----  ---  -----
  ----  --TS---  ---  -B--D--  ---STS  ----  RSQ  --C-- *DEFAULT
  ----  -------  ---  --S----  ------  ----  ---  ----- *TGLOBAL
  ----  -------  ---  --S----  ------  ----  ---  ----- *TPARMS
  ----  --TS---  DJ-  SSS-DFX  ---STS  ----  RSQ  --C-- TP-CURR
  ----  --TS---  DJ-  SSS-DFX  ---STS  ----  RSQ  --C-- FINAL
29 OF 29 RECORDS DISPLAYED
```

1 , **2** - CLIENTAUTH level 2 is being used for Certificate Express Logon.

3 - This is the RACF user ID associated to the client certificate.

Implementation of three-tier network design

The implementation of Certificate Express Logon with three-tier design is the same in both z/OS V1R2 and above and OS/390 V2R10. The following sections describe the implementation.

DCAS - DCAR connection

The Digital Certificate Access Server (DCAS) is a TCP/IP server that runs on OS/390 V2R10 and later. The middle-tier TN3270 servers connect to DCAS using Secure Socket Layers V3 (SSL). The purpose of DCAS is to receive an application ID and a digital certificate from a middle-tier TN3270 server, then ask RACF to return a valid user ID that has been associated with the certificate, and to generate a PassTicket for the input user ID and application ID.

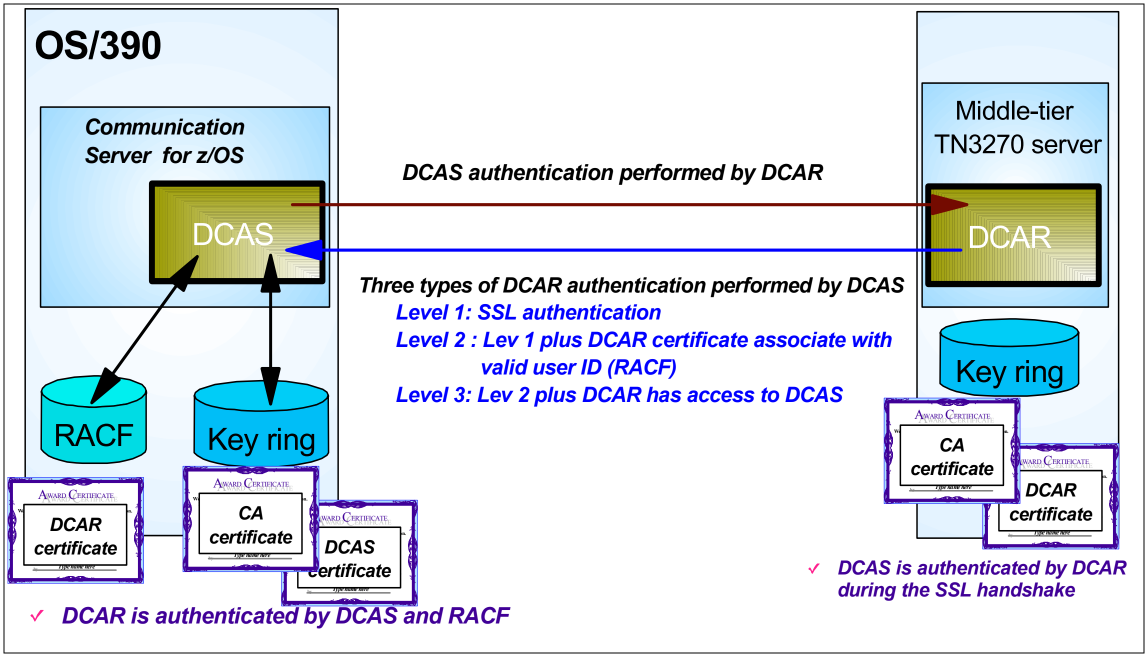

OS/390
Communication Server for z/OS
DCAS
RACF
Key ring
DCAR certificate
CA certificate
DCAS certificate
DCAS authentication performed by DCAR
Three types of DCAR authentication performed by DCAS
Level 1: SSL authentication
Level 2 : Lev 1 plus DCAR certificate associate with valid user ID (RACF)
Level 3: Lev 2 plus DCAR has access to DCAS
Middle-tier TN3270 server
DCAR
Key ring
CA certificate
DCAR certificate
✓ DCAS is authenticated by DCAR during the SSL handshake
✓ DCAR is authenticated by DCAS and RACF

Figure 3-6 DCAS/DCAR

Authenticating the Digital Certificate Access Server

The DCAS authentication is always performed by the Digital Certificate Access Requestor (DCAR) during the SSL handshake. Authentication requires that the DCAS has a private key and an associated X.509 digital certificate defined in a keyring.

If you use a self-signed certificate, it has to be treated as a CA certificate by all TN3270 servers. Follow these steps:

1. Export the DCAS self-signed certificate into a file in the DER binary format.
2. Send it to a TN3270 server, using FTP with the BINARY send option.
3. Store the certificate into a key database for the TN3270 server as a trusted Certificate Authority.

Authenticating the Digital Certificate Access Requestor

The DCAR is the client that interacts with the DCAS. Authenticating the DCAR involves additional levels of control in which the client must have a key database with a certificate. Depending on the control level, the certificate is authenticated by SSL and the DCAS using RACF services.

There are three levels of client authentication from which to choose:

- Level 1

  With Level 1 authentication, the DCAS uses the client authentication provided by SSL at the time of the SSL handshake. The keyring used by the DCAS must contain the following certificates:

  – The DCAS certificate

  – The certificate of a CA that has signed the TN3270 server certificate. Or, the TN3270 certificate itself, if a self-signed certificate is used for the TN3270 server.

  To configure DCAS for this level of authentication, specify the CLIENTAUTH LOCAL1 keyword in the DCAS configuration file. Use the KEYRING or the SAFKEYRING keywords in the DCAS configuration file to specify the keyring used by the DCAS.

- Level 2

  Level 2 includes Level 1 authentication plus additional verification that the DCAR certificate has been associated in RACF with a valid user ID. To configure DCAS for this level of authentication, specify the CLIENTAUTH LOCAL2 keyword in the DCAS configuration file. Use FTP (with the BINARY send option) to send the client's DER certificate to an MVS data set. Use the RACDCERT ADD command to add the certificate to RACF and associate it with a user ID, as shown in the following example:

  ```
  RACDCERT ID(dcasid) ASID('DCAS.DCAR.CERT') TRUST
  ```

- Level 3

  Level 3 includes level 2 authentication plus it verifies that the DCAR has access to the DCAS. The user ID derived from the certificate using the RACF checks from Level 2 is defined as having access to the SERVAUTH RACF class and the EZA.DCAS.cvtsysname resource in the SERVAUTH class. The following conditions apply:

  – If the SERVAUTH class is not active or the EZA.DCAS.cvtsysname profile is not defined, or both, it is assumed this enhanced level is not requested.

  – If the SERVAUTH class is active and the EZA.DCAS.cvtsysname profile is defined (but not for the user associated with the certificate) the requestor's connection is terminated.

  Use the commands below to create the RACF profile and give the access permission to a user:

  ```
  RDEFINE SERVAUTH EZA.DCAS.cvtsysname UACC(NONE)
  PERMIT EZA.DCAS.cvtsysname CLASS(SERVAUTH) ACCESS (CONTROL) ID(dcasid)
  SETR RACLIST(SERVAUTH) REFRESH
  ```

To configure DCAS for Level 3 authentication, follow these steps:

a. Specify the CLIENTAUTH LOCAL2 keyword and value in the DCAS configuration file.

b. Activate the SERVAUTH RACF class.

c. Define a profile for the EZA.DCAS.cvtsysname resource and associate the profile with the user ID associated with the certificate.

> **Note:** The ID associated with the certificate and the EZA.DCAS.cvtsysname can be any valid user ID.

DCAS customization

Follow these steps to customize DCAS for Certificate Express Logon with three-tier design:

1. Define an SSL session between DCAS (z/OS) and DCAR (middle-tier Telnet Server) and between DCAR and TN3270 client (Host On-Demand in our case). The procedure to define an SSL session is in "Configuring TCP/IP TN3270 server for SSL" on page 108. Instead of using the TCP/IP name, use the DCAS name on RACF commands.

   The user ID associated with the keyring and the DCAS server's certificate has to be the user defined in the STARTED procedure of DCAS.

   The DCAS certificate has to be imported into the key database used by the TN3270 server (middle-tier) and defined as trusted.

   The Host On-Demand client certificate has to be defined in RACF.

2. Set up DCAS to use RACF services.

   – Define started profile and OPERCMDS:

   ```
   ADDUSER DCAS DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/')

   RDEFINE STARTED DCAS.* STDATA(USER(DCAS))
   SETROPTS RACLIST (STARTED) REFRESH

   RDEFINE OPERCMDS(MVS.SERVMGR.DCAS) UACC(NONE)
   PERMIT MVS.SERVMGR.DCAS CLASS(OPERCMDS) ACCESS(CONTROL) ID(DCAS)
   SETROPTS RACLIST(OPERCMDS) REFRESH
   ```

   – Permit the DCAS to use certificate services:

   ```
   SETROPTS CLASSACT(DIGTCERT DIGTRING)
   RDEFINE FACILITY(IRR.DIGTCERT.LIST) UACC(NONE)
   RDEFINE FACILITY(IRR.DIGTCERT.LISTRING) UACC(NONE)
   PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(DCAS) ACCESS(CONTROL)
   PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(DCAS) ACCESS(CONTROL)
   SETROPTS RACLIST(DIGTRING DIGTCERT) REFRESH
   ```

- Define PassTicket data profile:

  ```
  SETROPTS CLASSACT(PTKTDATA)
  SETROPTS RACLIST(PTKTDATA)
  RDEFINE PTKTDATA TSORA03 SSIGNON(KEYMASKED(E6C9D30195D4C1E7)) UACC(NONE)
  SETROPTS RACLIST(PTKTDATA) REFRESH
  ```

3. Define DCAS configuration file.

   Some of the configuration parameters you can use in the DCAS configuration file are shown in Table 3-3.

Table 3-3 DCAS configuration parameters

Parameters	Description
IPADDR	Allows you to define the IP address to which the DCAS will bind.
PORT	Defines the port number on which DCAS will run.
KEYRING 1	Defines the HFS key database file containing the certificate to be used during the SSL handshake.
STASHFILE	Specifies the password file to the associate key database file.
SAFKEYRING 1	Defines the RACF-defined keyring containing the certificate to be used during the SSL handshake.
V3CIPHER	Specifies a subset of the supported SSL V3 cipher algorithms.

   1 - The keywords KEYRING and SAFKEYRING are mutually exclusive.

   Here is a sample DCAS configuration file that was used in the DCAS startup procedure for the next step:

   ```
   TCPIP TCPIPB
   PORT 8990
   CLIENTAUTH LOCAL2
   SAFKEYRING r2617.mvs28b.dcas.keyring 1
   # KEYRING /etc/dcas/dcas.kdb
   # STASHFILE /etc/dcas/dcas.sth
   ```

   1 - The keyring name is case sensitive

4. Start DCAS

   The following is a sample procedure for DCAS. It is also provided in hlq.SEZAINST(EZADCASP):

```
//DCAS PROC
//DCAS EXEC PGM=EZADCDMN,REGION=4M,TIME=NOLIMIT,
// PARM=('POSIX(ON) ALL31(ON)',
// 'ENVAR("_CEE_ENVFILE=DD:STDENV" ',
// '"DCAS_CONFIG_FILE=/etc/dcas.r2617.conf")/-d 3') 1
//CEEDUMP DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//STDENV DD DSN=TCPIP.TCPPARMS.R2617(DCASENV),DISP=SHR
```

1 - The DCAS configuration file is /etc/dcas.r2617.conf

By default DCAS writes the messages in the /tmp/dcas.log file. You can set the debug level in the **-d** start option.

When DCAS is started as an MVS started procedure, the following messages will show up in the MVS console:

```
S DCAS
$HASP100 DCAS ON STCINRDR
IEF695I START DCAS WITH JOBNAME DCAS IS ASSIGNED TO USER
TCPIP3 , GROUP OMVSGRP
$HASP373 DCAS STARTED
IEF403I DCAS - STARTED - TIME=20.36.55
EZZ8601I DCAS IS STARTING
EZZ8620I DCAS SECURITY SERVER SERVAUTH CLASS IS ACTIVE
EZZ8624I DCAS PROCESSING CONFIGURATION FILE /ETC/DCAS.R2617.CONF
EZZ8625I DCAS CONFIGURATION FILE PROCESSING IS COMPLETE
EZZ8618I DCAS LISTENING ON SECURE PORT 8990
```

5. Define a Host On-Demand TN3270 session and create a macro for Certificate Express Logon. Refer to 15.2.4, “Record the Logon macro” on page 587 for procedures for Host On-Demand or “Recording the Certificate Express Logon macro” on page 980 for Personal Communications Version 5.7 clients. The client setup is identical for two-tier and three-tier designs.

For more information about the Certificate Express Logon implementation with OS/390 V2R10 using the three-tier network design, refer to the following documents:

- *z/OS Communications Server IP Configuration Guide* for your operating system release
- *Communications Server for z/OS V1R2 TCP/IP Implementation Guide Volume 7: Security*, SG24-6840

3.8 LDAP directory server

The Lightweight Directory Access Protocol (LDAP) Server for OS/390 is part of the SecureWay® Security Server for OS/390 or z/OS. This server may be the LDAP Server for one or more Host On-Demand systems on any platform. The OS/390 LDAP server is configured in one of three modes: RDBM, SDBM or TDBM. Host On-Demand only works when the LDAP server is configured with a DB2® back-end database, RDBM, or TDBM. TDBM implementation, introduced with OS/390 Release 10, is the recommended implementation because it has an improved schema that includes the HOD required schema, and it uses a DB2 database that was designed for performance. For detailed information about the OS/390 LDAP Server, refer to the following:

- *OS/390 SecureWay Security Server LDAP Client Application Development Guide and Reference*, SC24-5878
- *OS/390 V2R10.0 SecureWay Security Server LDAP Server Administration and Usage Guide,* SC24-5861 for OS/390
- *z/OS Security Server LDAP Server Admin and Usage Guide*, SC24-5923 for z/OS

If you have an existing OS/390 Security Server, verify the following:

- The server is configured as described in the appropriate *SecureWay Security Server LDAP Server Administration and Usage Guide.*
- A suffix has been added and associated with an object class.

The remainder of this section focuses on the configuration of the OS/390 LDAP directory server. For information about using the LDAP server, refer to Chapter 8, “LDAP directory server” on page 373.

3.8.1 Schema installation

In order to use Host On-Demand with your existing LDAP directory, you will need to use the IBM schema shipped with the LDAP server. The process for setting up this schema is different for RDBM and TDBM.

Schema set up using RDBM backend

To add the IBM schema to the existing LDAP directory:

a. Edit the LDAP directory configuration file, slapd.conf, and modify the include statements as follows:

```
Original            IBM schema
____________________________________
slapd.at.system     schema.system.at
slapd.cb.at.conf    schema.IBM.at
slapd.at.conf       schema.user.at
slapd.oc.system     schema.system.oc
slapd.cb.oc.conf    schema.IBM.oc
slapd.oc.conf       schema.user.oc
```

b. Restart the LDAP directory server.

See the program directory for further information regarding DB2 tables.

Schema set up using TDBM backend

To add the IBM schema to the existing LDAP directory:

1. Use the **`ldapmodify`** command to add the `schema.user.ldif` that is shipped with the LDAP server.
2. Use the **`ldapmodify`** command to add the `schema.IBM.ldif` that is shipped with the LDAP server.

3.8.2 Directory tree

To configure an existing LDAP directory for Host On-Demand, familiarize yourself with the LDAP directory. Decide how Host On-Demand will fit into your network and organizational structure, and then design the LDAP directory information tree. For example:

- To build a directory information tree for an entire organization, use the organization object class for the suffix:

```
dn: o=MyOrganization
objectclass: organization
o: MyOrganization
```

- To build a directory information tree for one division of an organization, use the organizationalUnit object class for the suffix:

```
dn: ou=MyDivision, o=MyOrganization
objectclass: organizationalUnit
ou: MyDivision
```

The directory information tree should be defined in an LDAP Data Interchange Format (LDIF) file. Examples of the directory information tree can be found in /usr/lpp/ldap/examples/sample_server/sample.ldif. We created a file called itso.ldif with the following:

```
dn: ou=ITSO, o=IBM
objectclass: organizationalUnit
ou: ITSO
```

To add to the directory information tree in the LDAP directory, use the **ldapadd** command. The format of the **ldapadd** command is:

```
ldapadd -h <hostname> -p <port> -D “cn=<admin_id>,o=<organization>” -w
<password> -f <filename>
```

For example:

```
ldapadd -h bigtex.raleigh.itso.ibm.com -p 389 -D “cn=directory
manager,o=IBM” -w <password> -f itso.ldif
```

Compare this command to Figure 3-7 on page 127.

Details on using this command can be found in the *IBM SecureWay Security Server LDAP Client Application Development Guide and Reference*, SC24-5878.

3.8.3 Performance considerations

When using RDBM the following configuration changes are offered as possible performance enhancements that can be added to slapd.conf:

```
index pr nc palPtr eq
index dc eq
index o eq
index name eq
index objectClass eq
index u d eq
```

Sizelimit is a parameter in the `slapd.conf`. This is the number of entries the LDAP directory server will return on a search request; change the sizelimit to 5000 (this applies when using either RDBM or TDBM).

3.9 Native Authentication

The Native Authentication code runs as a separate executable module called *HODRAPD*, which is invoked using the **hodrapd.sh** shell script. The HODRAPD module is installed during SMP/E CALLLIBS processing, and it is automatically link-edited during the JCLIN CALLLIBS processing in the APPLY process.

When the Native Platform Authentication Service is started from UNIX System Services, the HODRAPD module is executed from SYS1.LINKLIB or your alternate LINKLIB data set. If you choose to move the HODRAPD module to an alternate LINKLIB data set, that data set must be accessed by the system LNKLST or LPALIB.

In order to use the Native Authentication service, Host On-Demand must enable an LDAP directory for the storage of preferences.

3.9.1 Installation of Native Authentication service

During installation of Host On-Demand V8, the **hod80mvs.sh** shell script not only untars the Host On-Demand V8 product, it also creates the necessary link so that when the user starts Native Authentication with **hodrapd.sh** shell script, the HODRAPD load module is executed. If the link to HODRAPD gets unlinked, the statements below can be used to restore the link.

Example 3-21 Restore link for HODRAPD

```
export HOD_DIR=/usr/lpp/HOD
touch $HOD_DIR/hostondemand/private/HODRAPD
ln -s $HOD_DIR/hostondemand/private/HODRAPD (continued on next line)
$HOD_DIR/hostondemand/private/hodrapd
chmod 744 $HOD_DIR/hostondemand/private/HODRAPD
chmod +t $HOD_DIR/hostondemand/private/HODRAPD
```

The Native Authentication code logs its messages to the syslog, which may need to be configured to log the desired level of messages. The HODRAPD module writes its messages to the user.* entry in the syslog.conf file.

3.9.2 Starting Native Authentication service

To start the Native Authentication code, run the **hodrapd.sh** shell script (located in the /usr/lpp/HOD directory). The shell script may need to be edited if you installed Host On-Demand in a directory path other than /usr/lpp/HOD.

The shell script also has options that can be set. Options such as logging, time-out values, and maximum number of requests the server will allow can be specified when you start the service. You must keep the **-x** option, but can append any of the following options. Edit the line where the HODRAPD module is called, and append the following options if desired:

l Enable logging (for example, **-xl**)

t Set socket timeout value, in seconds, default is 20 (for example, **-xt100**)

c Set the max number of requests the server will allow (for example, **-xc100**)

The shell script must be started by a user with root authority.

HODRAPD can be started from the OMVS shell or as a started task. To start HODRAPD from the from OMVS shell, go your Host On-Demand install directory and run the shell script. For example:

```
cd /usr/lpp/HOD
hodrapd.sh
```

The following is a sample procedure we used to start HODRAPD.

Example 3-22 Sample HODRAPD started procedure

```
//HODRAPD PROC
//* HOST ON DEMAND VERSION 7
//HODSRVG EXEC PGM=BPXBATCH,REGION=0M,TIME=NOLIMIT,
//      PARM='sh /usr/lpp/HOD/hodrapd.sh'
//SYSPRINT DD SYSOUT=A
//SYSERR   DD SYSOUT=A
//SYSOUT   DD SYSOUT=A
//STDENV   DD DSN=TCPIPOE.SC48.TCPPARMS(HODENV),DISP=SHR
//SYSIN    DD DUMMY
//STDOUT   DD PATH='/tmp/HODRAPD.stdout',
//          PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//          PATHMODE=SIRWXU
//STDERR   DD PATH='/tmp/HODRAPD.stderr',
//          PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//          PATHMODE=SIRWXU
```

Because our system had more than one TCP/IP stack, we had to make sure the HODRAPD task established affinity to the correct stack. We set the following environment variable in the data set member pointed to by DD name STDENV:

```
_BPXK_SETIBMOPT_TRANSPORT=TCPIPOE
```

When the Native Authentication service is completely started, a message is displayed on the z/OS console unless you have logging enabled. Then it is displayed in the syslog. The message reads:

```
PAS0001 Starting IBM Platform Authentication Service.
```

You can check the status of the Native Authentication service by issuing the **netstat conn** command from TSO or **netstat -a** from USS (UNIX System Services). The command will display the status of the service. The Native Authentication service uses the well-known port 2569. The **netstat** command will display the following status based on the user ID for the Native Authentication service:

```
   MVS TCP/IP onetstat CS V2R10       TCPIP Name: TCPIPOE          11:03:39
   User Id  Conn     Local Socket           Foreign Socket         State
   -------  ----     ------------           --------------         -----
   HODRAPD2 00005CCE 0.0.0.0..2569          0.0.0.0..0             Listen
```

If the port is not in listening status, verify the permissions of HODRAPD in the private directory. The file must have the sticky bit turned on as shown below:

```
   -rwxr--r-T   1 AAAAAAA  SYS1            0 Dec  8  2000 HODRAPD
```

If the sticky bit (denoted by the T) is not set, use the **chmod** commands shown in Example 3-21 on page 124 to set the bit.

When the Native Authentication service is started, two UNIX System Services processes are started as shown in Example 3-23.

Example 3-23   HODRAPD process IDs

```
UID        PID       PPID  C    STIME TTY       TIME CMD
 AAAAAAA   50332132   33554917  - 10:34:41 ?         0:00 hodrapd -xl
 AAAAAAA   33554917          1  - 10:34:39 ?         0:00 hodrapd -xl
```

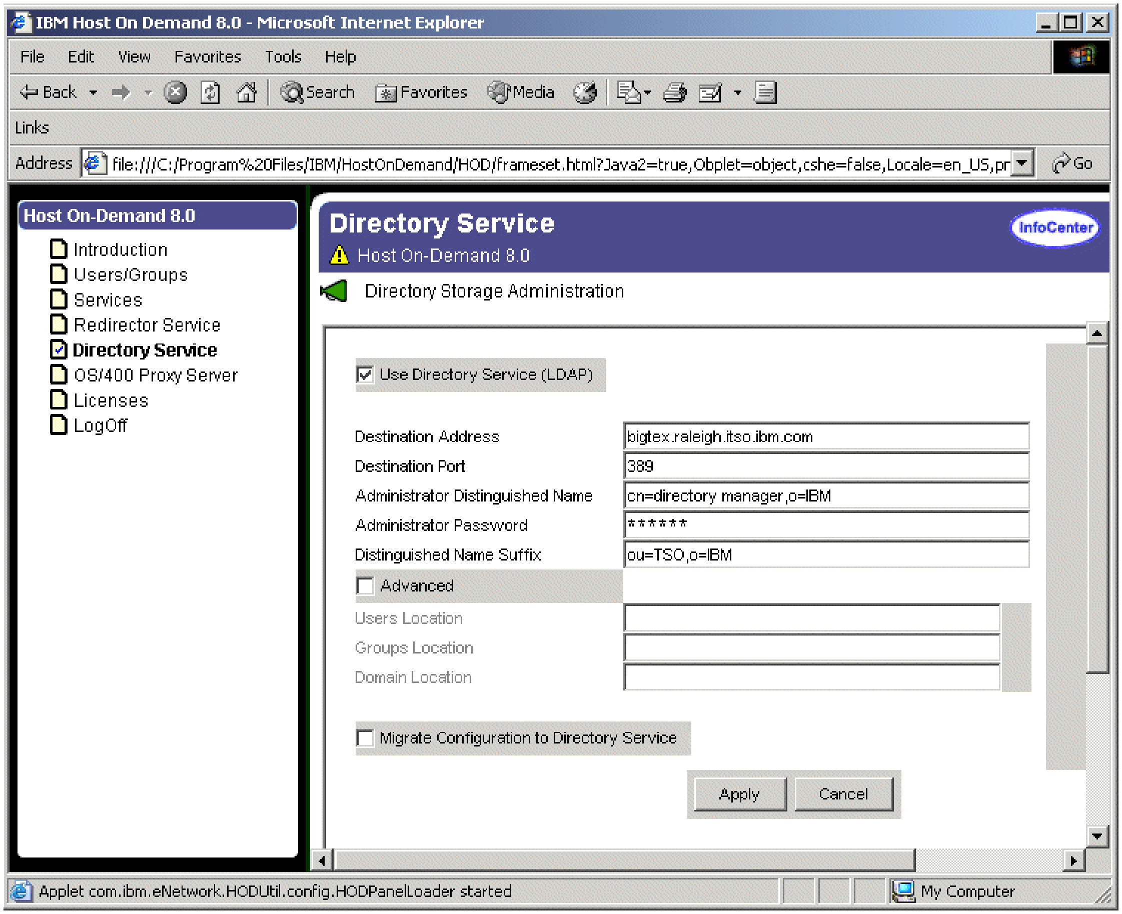
The **hodrapd.sh** shell script appends to your LIBPATH and NSLPATH. You may want to append these statements to your `/etc/profile` in USS. For example:

```
   export NLSPATH=$NLSPATH:/usr/lpp/HOD/hostondemand/lib/msgs/%N
   export LIBPATH=$LIBPATH:/usr/lpp/HOD/hostondemand/lib/
```

3.9.3 Testing Native Authentication service

In order to verify that the Native Authentication service is working correctly, perform the following steps:

1. Log on to the Host On-Demand administrator and insure that the LDAP directory is enabled as shown in Figure 3-7.



Directory Service

Host On-Demand 8.0

Directory Storage Administration

☑ Use Directory Service (LDAP)

Destination Address	bigtex.raleigh.itso.ibm.com
Destination Port	389
Administrator Distinguished Name	cn=directory manager,o=IBM
Administrator Password	******
Distinguished Name Suffix	ou=TSO,o=IBM

□ Advanced

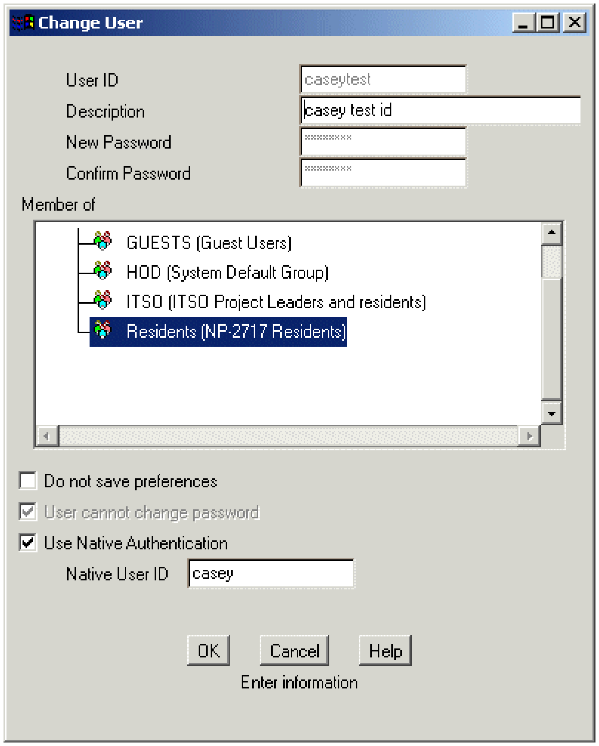
Users Location	
Groups Location	
Domain Location	

□ Migrate Configuration to Directory Service

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 3-7 Using Directory Service

2. Verify that Native Authentication is enabled for at least one user by selecting **Use Native Authentication** and providing a native user ID as shown below.
3. Click **OK**.
4. Log off the Host On-Demand administrator.
5. Download a Host On-Demand client, and log onto the ID using the password of the Native user ID that you specified. Using the example above, the Host On-Demand user ID is CASEYTEST and the password is the RACF password of native ID CASEY.



User ID caseytest

Description casey test id

New Password ********

Confirm Password ********

Member of

- GUESTS (Guest Users)
- HOD (System Default Group)
- ITSO (ITSO Project Leaders and residents)
- Residents (NP-2717 Residents)

☐ Do not save preferences

☑ User cannot change password

☑ Use Native Authentication

Native User ID casey

Enter information

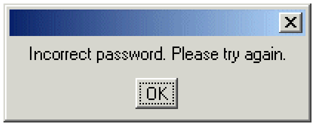
Figure 3-8 Enabling Native Authentication

Problem determination

If you receive an invalid logon (Figure 3-9) and you know without a doubt that the user ID and password is correct, verify you have defined localhost in the /etc/hosts file. You must be able to resolve localhost. If necessary, add an entry for `localhost` as follows in the /etc/hosts file:

```
127.0.0.1     localhost
```

If you make a modification to the /etc/hosts file, you must recycle the Host On-Demand server. The HODRAPD task does not need to be recycled.



Incorrect password. Please try again.

Figure 3-9 Native Authentication logon failure

Stopping the Native Authentication service

When the service is started, two UNIX System Services processes are started as described in 3.9.2, “Starting Native Authentication service” on page 124. The service can be stopped in one of two ways. Both ways require that you determine the PID of the first process that is started. From the OMVS shell, issue the **`ps -ef`** command or from the MVS console issue **`d omvs,a=all`** and find the two processes. Using Example 3-23 on page 126, the HODRAPD service can be stopped with either of the following commands:

- From OMVS shell:

  ```
  kill -9 33554917
  ```

- From the MVS console:

  ```
  f bpxoinit,term=33554917
  ```

4

iSeries tips

In this chapter, we cover some of the top OS/400-related tips and techniques from the Host Access Call Center Team, including:

- The iSeries as a Host On-Demand server
- Performance tips
- Other iSeries tips

4.1 Upgrading the JVM level to 1.3

Some modest performance gains can be obtained by using the most advanced Java release level. However, some applications are not compatible with this level just yet. OS/400 can support multiple JVM levels, here are the steps:

1. As new JVM levels are announced, they will become available through PTFs. Refer to:

   `http://www-912.ibm.com`

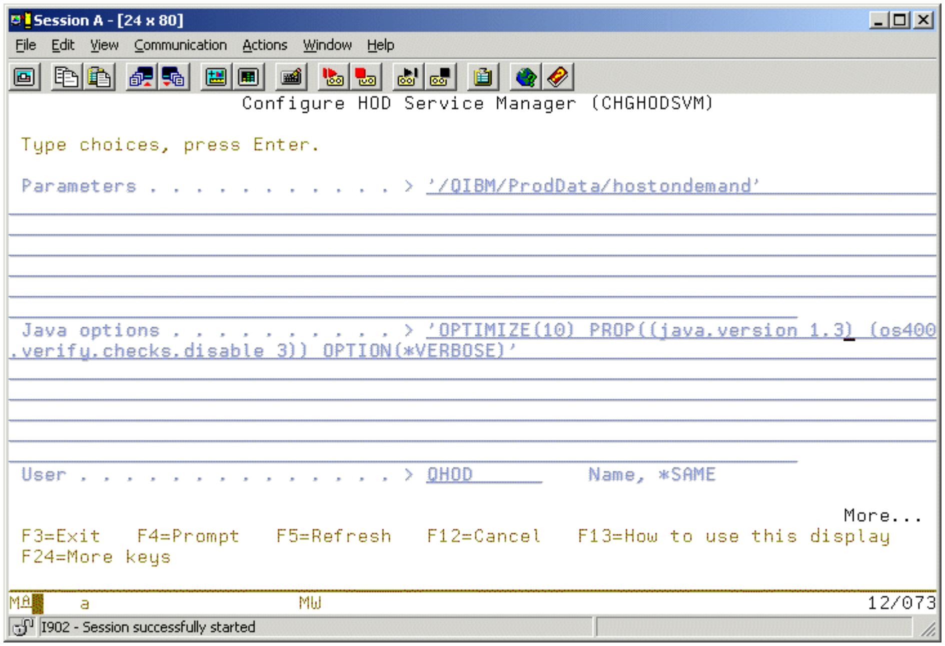
   You may also want to obtain the latest Java group PTF and cumulative service.

Table 4-1 Current OS/400 PTFs

OS/400 level	Java Group PTF	JVM 1.3 PTF
V4R4	SF99067	SF63322
V4R5	SF99068	SF63319
V5R1	SF99069	*
V5R2	SF99169	*
*** = included with base CD set for OS/400**		

2. Install the JVM. Even though the CD is distributed as a PTF, the installation instructions will tell you to use the `RSTLICPGM` command.
3. Apply the Cumulative Service CDs by choosing **option 8** on the GO PTF menu.
4. Apply the Java Group PTF CD by choosing **option 8** on the GO PTF menu.
5. Adjust Host On-Demand to use JVM 1.3 the next time it is started:
   - CFGHODSVM
   - Page down
   - Add the property (java.version 1.3) to the Java options as shown in Figure 4-1 on page 133.
   - Press Enter.
6. Restart the Host On-Demand Service Manager:
   - ENDHODSVM
   - STRHODSVM
7. Validate that JVM 1.3 is being used:
   - WRKJOB QHODSVM
   - Choose the active job.
   - Select **option 4** to view printouts for the job.

- Select **option 5** to view the printout.
- The message `Finding native method library: QJAVA QJVIO13` indicates that the 1.3 JVM is being used.



```
                   Configure HOD Service Manager (CHGHODSVM)

 Type choices, press Enter.

 Parameters . . . . . . . . . . . > '/QIBM/ProdData/hostondemand'







 Java options . . . . . . . . . . > 'OPTIMIZE(10) PROP((java.version 1.3) (os400
.verify.checks.disable 3)) OPTION(*VERBOSE)'





 User . . . . . . . . . . . . . . > QHOD          Name, *SAME

                                                                       More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
MA      a                        MW                                     12/073
I902 - Session successfully started
```

Figure 4-1 Switching JVM to 1.3

4.2 Using IBM HTTP Server (Powered by Apache)

The trend for OS/400 is to switch from the 5769-DG1 HTTP server to the Apache server. Customers may have switched their default Web instances and would like to handle Host On-Demand with Apache.

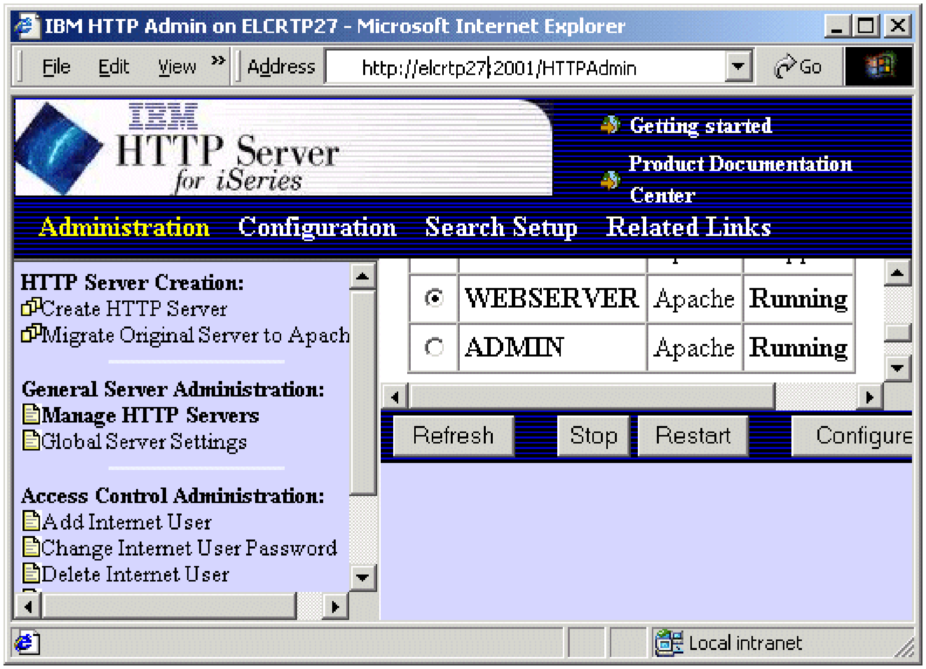
The following describes how to add the “hod” directive to an existing Apache Web instance. For the latest information on the HTTP server (powered by Apache), refer to:

http://www.ibm.com/servers/eserver/iseries/software/http/services/apache.htm

1. From a browser, start the main Web page for your iSeries:

   `http://<system.name>:2001/HTTPAdmin` (if you are using V5R1 or V5R2)
   `http://<system.name>:2002/HTTPAdmin` (if you are using V4R5)

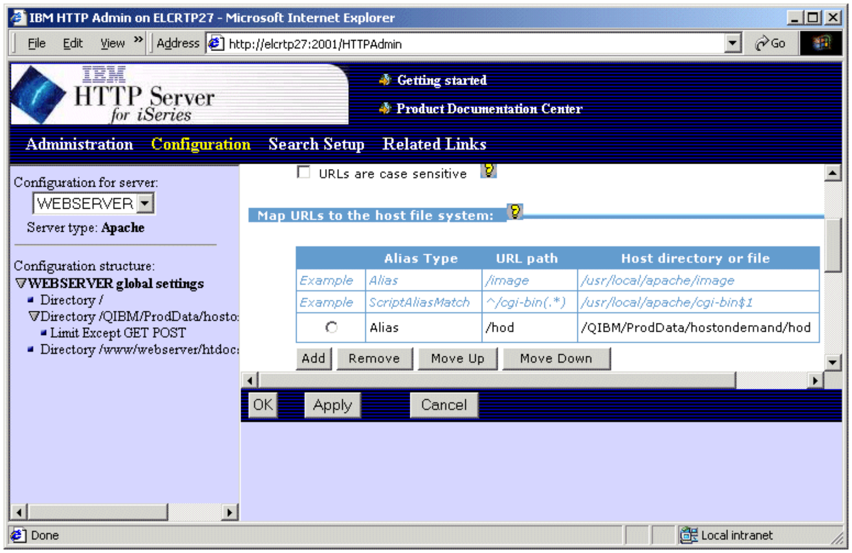
2. Click **Manage HTTP Servers** under General Server Administration. See Figure 4-2.


IBM HTTP Admin on ELCRTP27 - Microsoft Internet Explorer
File Edit View Address http://elcrtp27:2001/HTTPAdmin Go
IBM HTTP Server for iSeries
Getting started
Product Documentation Center
Administration Configuration Search Setup Related Links
HTTP Server Creation:
Create HTTP Server
Migrate Original Server to Apach
General Server Administration:
Manage HTTP Servers
Global Server Settings
Access Control Administration:
Add Internet User
Change Internet User Password
Delete Internet User
Refresh Stop Restart Configure
Local intranet

●	WEBSERVER	Apache	Running
○	ADMIN	Apache	Running

Figure 4-2 Starting the iSeries Apache Configuration tool

3. Select the instance that you want to update. In this case, we are updating the WEBSERVER Apache instance (the root directory is /www/webserver).
4. The configuration window is shown for the WEBSERVER instance. Click the **Aliases and Redirection** link.



Configuration for server: WEBSERVER

Server type: **Apache**

Configuration structure:

▽**WEBSERVER global settings**
- Directory /
- ▽Directory /QIBM/ProdData/hosto
  - Limit Except GET POST
- Directory /www/webserver/htdoc

□ URLs are case sensitive

Map URLs to the host file system:

	Alias Type	URL path	Host directory or file
Example	*Alias*	*/image*	*/usr/local/apache/image*
Example	*ScriptAliasMatch*	*^/cgi-bin(.*)*	*/usr/local/apache/cgi-bin$1*
○	Alias	/hod	/QIBM/ProdData/hostondemand/hod

Figure 4-3 Adding the /hod alias

5. Click **Add** in the Map URLs to the host file system section. Then select **Alias**. Set the URL path to `/hod` and the Host directory to `/QIBM/ProdData/hostondemand/hod`. Finally, click **OK**.

6. Click **Edit Configuration File** (located in the bottom right). Add the following text lines to the configuration just before the <Directory /> line:

```
<Directory /QIBM/ProdData/hostondemand/hod>
   <LimitExcept GET POST>
   order deny,allow
   deny from none
   </LimitExcept>
   AllowOverride None
   UseCanonicalName Off
   HostNameLookups off
   Options +FollowSymLinks
</Directory>
```

7. Click **OK**. You will return to the instance configuration window.

8. Click **Restart**. In a few moments, you should be able to bring up the `http://as400/hod/hodmain.html` window.

9. An interesting option that you may want to consider is to require the user to sign on to the HTTP server. This can be accomplished by replacing the information entered in Step 6 above with the following:

```
<Directory /QIBM/ProdData/hostondemand/hod>
   PasswdFile %%SYSTEM%%
   AuthType Basic
   UserID %%CLIENT%%
   AuthName usr
   require valid-user
   <LimitExcept GET POST>
   Order allow,deny
   Allow from none
   </LimitExcept>
   AllowOverride None
   UseCanonicalName Off
   HostNameLookups off
   Options +FollowSymLinks
</Directory>
```

4.3 Using Lotus Domino HTTP Server

Some customers have a Domino HTTP server as their default server or may want users to authenticate to their Domino HTTP server before any Web pages are served.

The following instructions were tested on Lotus Notes® for iSeries Release 5.04. Refer to the *Getting Started with Lotus Notes for iSeries 5.07* manual, which will guide you in configuring your server so that a basic Web page can be served.

This example assumes that you have previously installed the Domino Administrator tool on a PC. On the PC, perform the following steps.

1. Click **Start -> Programs -> Lotus Applications -> Lotus Domino Administrator**.
2. Click **File -> Tools -> User id** (choose the user ID for the Domino administrator).
3. Click **File -> Open server -> <specify server name> -> OK**.
4. A window similar to Figure 4-4 will be shown.

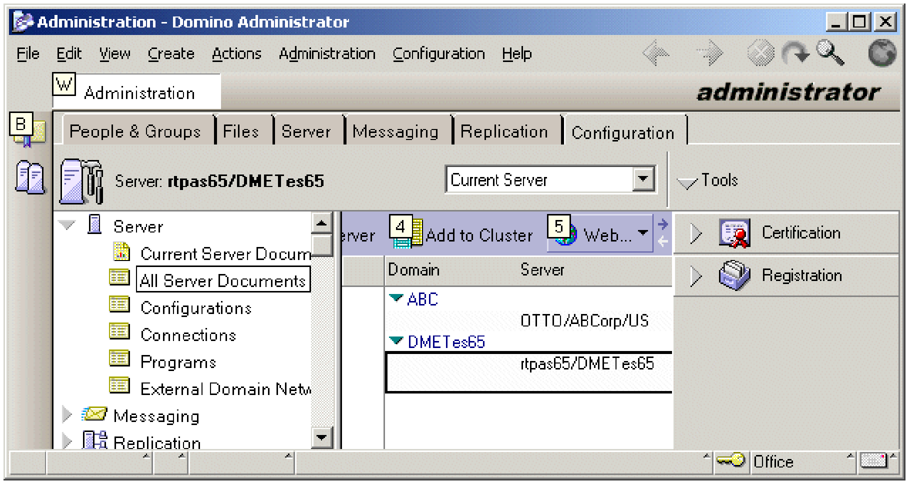
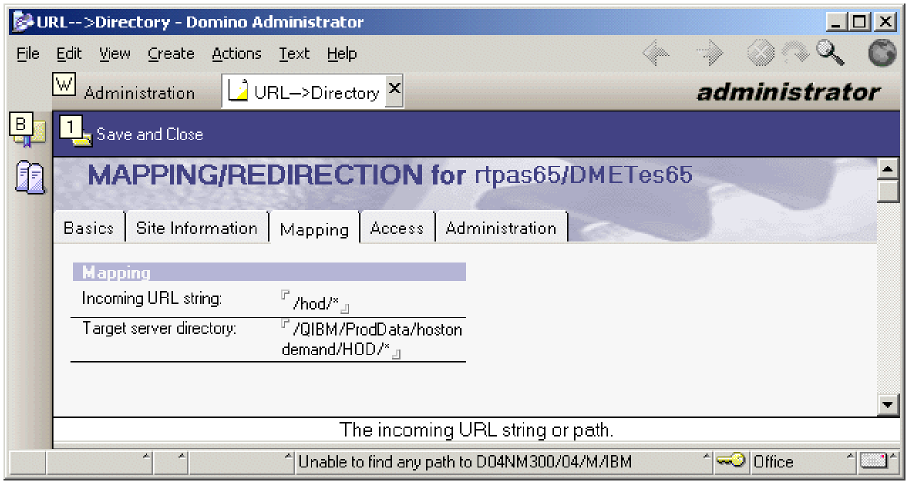


Figure 4-4 Starting the Domino Administration tool

5. Click the **Configuration** tab.
6. Open the server documents.
7. Click **All Server Documents**.
8. Find the server you wish to update. In the example below, we chose the **DMETes65** system.
9. Click the **Web...** action on the menu bar (its icon is a globe symbol). Note that you may have to use the (**->**) left arrow on the action bar to view the icon if your screen is limited in size.
10. Click **URL mapping**.
11. Leave the settings for the Basics and Site Information fields blank (so that the information applies to all Virtual Servers). Click the **Mapping** tab. A window similar to Figure 4-5 will be displayed.



MAPPING/REDIRECTION for rtpas65/DMETes65

Mapping

Incoming URL string: /hod/*

Target server directory: /QIBM/ProdData/hostondemand/HOD/*

The incoming URL string or path.

Unable to find any path to D04NM300/04/M/IBM

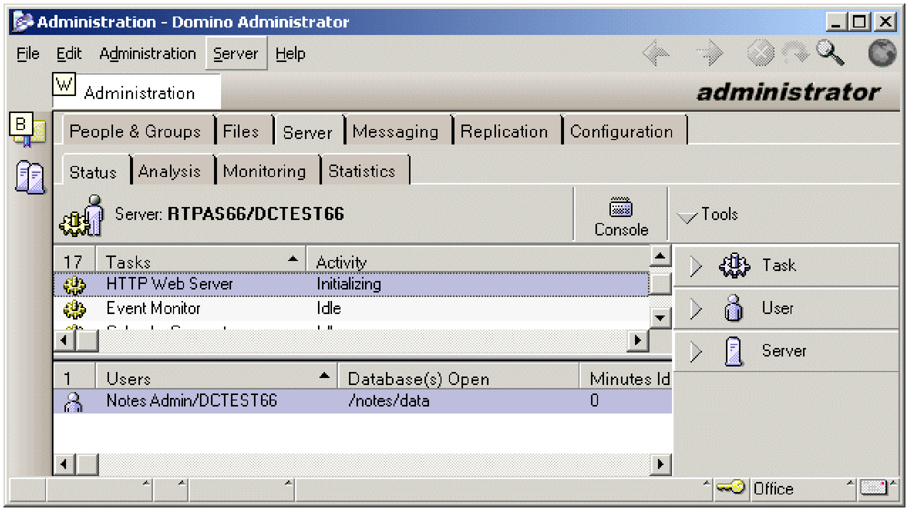
Figure 4-5 Specify the map to the Host On-Demand directory

12. Type `/hod/*` for the Incoming URL string (see Figure 4-5).
13. Type `/QIBM/ProdData/hostondemand/hod/*` in the Target server directory field.
14. Click **Save** and **Close**.

4.3.1 Restarting the Domino HTTP Server

The Web server must be restarted before the new directive becomes effective. The following procedure will cause a quick restart:

1. Click the **Server** tab.
2. Locate the HTTP Web Server task as shown in Figure 4-6.



Server: **RTPAS66/DCTEST66**

17	Tasks	Activity
	HTTP Web Server	Initializing
	Event Monitor	Idle

1	Users	Database(s) Open	Minutes Id
	Notes Admin/DCTEST66	/notes/data	0

Figure 4-6 Restarting the Domino HTTP server

3. Click the **Server** menu option on the top bar.
4. Click **Task -> Tell -> Restart HTTP server -> Clear cache**.

4.3.2 Using the Domino HTTP Server and Host On-Demand

The typical Host On-Demand Web pages should serve in a manner similar to the DG1 product. For example, `http://rtpas65/hod/hodmain.html`.

4.4 Using the configuration servlet

An installation script has been provided to install the Host On-Demand configuration servlet. Additional information on the Host On-Demand configuration servlet can be found in Chapter 9, “Configuration servlet” on page 387.

Installation notes:

- WebSphere V4.0 or V3.5 must be installed and the subsystem must be active. Advanced, Standard or Advanced Edition Single Server versions are supported.
- WebSphere security must be temporarily disabled.
- To install:

  a. Run **`qsh`**

b. Enter `cd /qibm/proddata/hostondemand/lib/samples/HodServlet`

c. Run **`CfgHodServlet-OS400.sh`**

- **Note:** You may optionally specify a WebSphere instance using the -instance xxx parameter. If the parameter is not specified, the instance is assumed to be default.
- The installation script may run for a minute or two. The installation program is complete when a dollar sign ($) is shown.

d. Exit from **`qsh`** by pressing F3.

e. Run **`EDTF`** '**`/QIBM/ProdData/hostondemand/hod/config.properties`**'

f. Add the following line:

```
ConfigServerURL=/HODServlet/HODServlet/hod
```

g. Press Enter, then press F3 to update the config.properties file.

h. Start the WebSphere Application Server instance. Refer to the WebSphere Getting Started Manual for additional details.

i. Restart the Host On-Demand service manager:

- ENDHODSVM
- STRHODSVM

being careful that you enter `/HOD` in uppercase.

- Attempt to use the Web page `http://my400/`**`HOD`**`/hodmain.html`.

  Be very careful that you enter `/HOD` in uppercase.

- For faster execution, consider the method discussed in 4.6.2, "Compile Host On-Demand for faster execution" on page 142.

4.5 Adding a printer definition table entry

A printer definition table allows a custom printer to be created. To create a new printer definition table, perform the following steps:

1. Map a network drive to the iSeries. See 4.7.4, "Mapping a network drive to the iSeries" on page 145.

   ```
   net use z: \\my400.ibm.com\hodpdt /user:bob
   ```

2. Use a text editor to create a definition file. Type the following after clicking **Start -> Run** on your PC:

   ```
   notepad z:\newprt.pdf
   ```

3. Use a text editor to modify the script. Type the following after clicking **Start -> Run** on your PC:

notepad z:\pdtcompilerapplication-OS400

- Locate the word NONGUI_COMMAND.
- Add a new line:
  NONGUI_COMMAND='newprt.pdf "my description" '

4. Compile the newprt.pdt file. Type the following OS/400 commands:
   - **qsh**
   - **cd /qibm/proddata/hostondemand/hod/samples**
   - **cd pdtcompilercommandfiles**
   - **PdtCompilerApplication-OS400**

   > **Important:** PdtCompilerApplication-OS400 is case sensitive. Enter the code as shown.

For additional information, refer to Chapter 21, "Printing" on page 713 for more information on 5250 Host Print, and to the online *Host Printing Reference* document.

4.6 Performance tips

By following the suggestions in this section, you should be able to improve the overall performance of your iSeries Host On-Demand system.

4.6.1 Web page caching

We found that when using the original iSeries Web server, 5769-DG1 and 5722-DG1 HTTP server, Host On-Demand can utilize the HTTP server "local caching" feature (57% performance improvement in hits/sec/CPW). A read from main memory is much faster than accessing the object from disk. However, if memory is being required by a system process, the objects will be paged out, which negates the performance gains. Refer to *AS/400 HTTP Server Performance and Capacity Planning,* SG24-5645 for additional details.

To enable Web caching for "original" iSeries Web instances:

1. WRKHTTPCFG
2. Add the following directives:
   - CacheLocalMaxBytes 100 M
   - LiveLocalCache On
   - CacheLocalFile /QIBM/ProdData/hostondemand/hod

To enable Web caching for iSeries Web instances "powered by Apache":

1. Start the Administration Web page. See 4.2, “Using IBM HTTP Server (Powered by Apache)” on page 133 for details.
2. Click the **Global Settings** link in the left menu panel. See Figure 4-2 on page 134.
3. Click the **Performance** link near the bottom of the menu.
4. Under the “Files to cache when server is started” section, click the **Add** button.
5. Type `/QIBM/ProdData/hostondemand/HOD/*`, then select **Copy into memory**.
6. Since the information in the HOD directory is stable, the normal setting for *Dynamically cache files based on file usage* is `off`.
7. *Update cache when files are modified* is normally set to `on`.
8. Click **OK**, then click the **Restart** button for the Web instance.

4.6.2 Compile Host On-Demand for faster execution

The largest performance gain we noticed was achieved by installing the JVM 1.3. See 4.1, “Upgrading the JVM level to 1.3” on page 132. Starting with OS/400 V4R5 and higher, Java will automatically perform Just In-Time compilation.

To create a more efficient environment, OS/400’s JVM compiles Java classes into native code as they are loaded. However, since the compilation process can be lengthy, depending on the number of classes and the size of the ZIP and JAR files, this may not be desirable because it will take a long time to start a session or load a function.

To avoid a delay and provide good performance, you should compile the class files, ZIP files, and JAR files immediately after installation. This also allows for better optimization between classes within packages.

The files to compile are:

- sm.zip
- ods.jar (see note below)
- jndi.jar
- ibmjndi.jar
- jsdk.jar
- cfgsrvlt.jar (only if you are planning to use WebSphere configuration servlet)

All of the files reside in /QIBM/ProdData/hostondemand/lib.

To compile the files, run a command similar to the following for each file except ods.jar:

```
CRTJVAPGM CLSF('/QIBM/ProdData/hostondemand/lib/sm.zip') OPTIMIZE(30)
```

Note that the ods.jar files requires an additional option. In prompt mode for the command **CRTJVAPGM**, press F10 for additional parameters, and in the field labeled Licensed Internal Code options, replace `*optimize` with `errorreporting=2`. This option is only available on V4R3 and later. The syntax for the command line option is:

```
CRTJVAPGM CLSF('/QIBM/ProdData/hostondemand/lib/ods.jar') OPTIMIZE(30)
LICOPT('errorreporting=2')
```

Optimization can take a long time and uses a lot of processor capacity. It depends on many conditions, including the power of the iSeries and what else it is doing at the time. It is best done when the machine is not busy with other tasks.

4.7 iSeries as a target host

The following tips are for use when the iSeries is the target host system.

4.7.1 5250 Workstation ID

Starting with Host On-Demand V 5.04, Host On-Demand supports some special values for workstation ID (device name). This allows Host On-Demand 5250 Display and Printer Sessions to generate a non-arbitrary device name for a session without requiring per-session customization or a user exit.

Table 4-2 Special values for 5250 workstation ID

Character	Function	Example string	Example devices
*	Short Session ID	A123*	A123A, A123B

%	Session type:
	S=display
	P=printer
		%DEV	SDEV

=	Collision avoidance. If device is in use, generate.	%DEV=	If SDEV1 is in use, then try SDEV2, etc. until successful

&COMPN	Computer name obtained from TCP settings.	&COMPN%=
		(MYPC=computer
		S=display
		A=short ID)
			MYPCSA

Character	Function	Example string	Example devices
&USERN	User name. (Windows clients only)	&USERN%= (BOB=user, S=display, A=short ID)	BOBSA
+	Trim the excess from the right side.	+&COMPN (computer= CLIENTACCESS	

If the resulting device name exceeds ten characters, the excess will be trimmed from the left side. This produces fewer duplicate device names for “left to right” languages, such as English. Excess characters can alternatively be trimmed from the right side by prefixing the CN keyword with a plus sign character (for example, `+&COMPN`).

Restrictions:

- A numeric character in the first position of a DEVNAME is invalid, and may be converted by OS/400 to the `#` (pound or hash) character.
- This is only supported on Win32 platforms.

4.7.2 5250 Telnet dropout

If you are using a firewall, make sure that the firewall inactivity time-out value for Telnet connections is at least as long as the session keep alive timeout (TIMMRKTIMO) parameter on the **`CHGTELNA`** OS/400 command.

4.7.3 Tip for 5250 printing

The first time an output queue is used, a `CPA3394` (“`Load form type ‘*STD’ in device xxx`”) message is directed to the message queue for the OUTQ. The message must be answered before the printouts begin to print.

Caution: If you use the `autoreply` command below, the feature is automatically set for all printers for the iSeries. When `autoreply` is activated, the printer will not prompt the printer operator for form changes.

To automatically have the system answer the message, use the following command:

```
ADDRPYLE SEQNBR(9999) MSGID(CPA3394) RPY(G)
```

4.7.4 Mapping a network drive to the iSeries

The iSeries can participate in a Windows Network Neighborhood. It may be helpful to create the following shares.

Table 4-3 Typical shares for Host On-Demand

Share	Target directory	Used for
hodpubl	/QIBM/ProdData/hostondemand/hod	Publish custom Web pages using the Deployment Wizard.
hodpdt	/QIBM/ProdData/hostondemand/hod/samples /PdtCompilerCommandFiles	Publish printer definition tables.

Tip: When you attempt to map a network drive to the iSeries, the Windows user ID and password must match your iSeries user ID and password. If your workstation operating system is Windows NT or Windows 2000, you may click **Connect using a different user name** on the Map Network Drive.

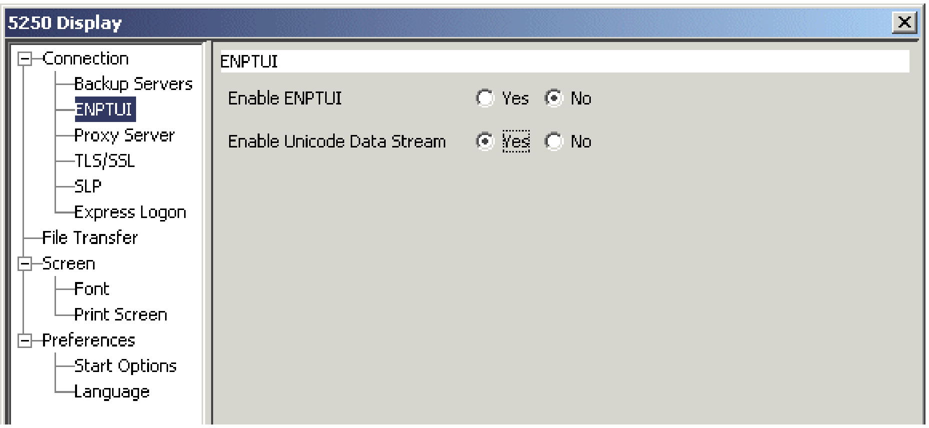
For additional information, refer to:

http://www.ibm.com/servers/eserver/iseries/netserver

4.7.5 Unicode support for OS/400

For 5250 Display sessions, Host On-Demand supports iSeries hosts that send Unicode data using tagged Coded Character Set Identifiers (CCSID) fields. This enhancement allows Unicode data to be displayed in 5250 Display sessions. It is not supported on a 5250 Printer Session.

In order to use this function, you will need to have both host application and client to handle unicode support. For host application, you will need to have one which handles unicode. For the Host On-Demand client, select **Yes** for **Enable Unicode Data Stream** in the Enhanced Non-Programmable Terminal User Interface (ENPTUI) section of 5250 Display properties.



ENPTUI

Enable ENPTUI ○ Yes ● No

Enable Unicode Data Stream ● Yes ○ No

Figure 4-7 Set Enable Unicode Data Stream for 5250 Display session properties

Host On-Demand supports the following CCSIDs. For any other CCSID, Host On-Demand will return a sense code of 0x10050155 in response:

- 13488 (hexadecimal 0x34B0)
- 17584 (hexadecimal 0x44B0)

Requirements

The following are the requirements for server and client.

Requirements on server

The iSeries host must be running one of the following levels of OS/400:

- OS/400 V5R2 with following PTFs
  - SI08903
  - SI08904
  - SI08933
  - SI08985
- OS/400 V5R3 or higher

Requirements on clients

There are several requirements for client machine to use this feature:

- For Bidi languages:
  - Java 2 and Web Start client
  - Use the Courier New font that is already installed on the client workstation.
- For other languages:
  - Java 1, Java 2, and Web Start client

  - The client machine must be configured to use one of the Monotype Sans Duospace WT fonts.

For more information on client configuration, refer to *Host On-Demand V8 Infocenter,* and the section titled *"Unicode support for OS/400 using Coded Character Set Identifiers."*

For information on host programming information, please refer to:

```
http://publib.boulder.ibm.com/pubs/html/as400/infocenter.html
```

Limitations

The following limitations apply to Unicode support on OS/400:

- A SBCS session supports only single-width Unicode characters.
- A DBCS session supports both single-width Unicode and double-width Unicode characters:
  - Supports only double-width Unicode character that are included in the Monotype Sans Duospace WT font file corresponding to the code page that the session is using.
- The following codepage or characters are not supported:
  - Hindi codepage
  - Thai codepage
  - Tamil Unicode characters
  - Teluga Unicode characters
  - Tibetan Unicode characters
  - Mongolian Unicode characters
  - Surrogate Unicode characters (these characters are accepted, but are displayed incorrectly by Java).
- GB18030 Phase 1 is already supported by Host On-Demand. This feature does not imply support for GB18030 Phase 2.
- This feature does not support any combining characters in CCSID-based entry field and output data.
- This feature does not support Language Tags (Plane 14) of UTF-16, because Host On-Demand does not support multiple fonts within one session.

4.7.6 Additional iSeries-related Web pages

Table 4-4 lists some useful iSeries Web pages.

Table 4-4 Additional iSeries related Web pages

Title	Web page
Common SSL problems. Also has a table describing the Telnet-SSL return codes	`http://publib.boulder.ibm.com/iseries/v5r1/ic2924/tstudio/tech_ref/tcp/telntssl/Index.htm`
Telnet exits-filter Telnet service by IP address	`http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzaiw/rzaiwmantelsrvr.htm`
National Language exit - ADDNLS tool	`http://publib.boulder.ibm.com/iseries/v5r1/ic2924/tstudio/tech_ref/tcp/telex/telexdwn.htm`
iSeries Performance Estimator Tool	`http://publib.boulder.ibm.com/pubs/html/iseries/online/chgfrm.htm`

5

Clients

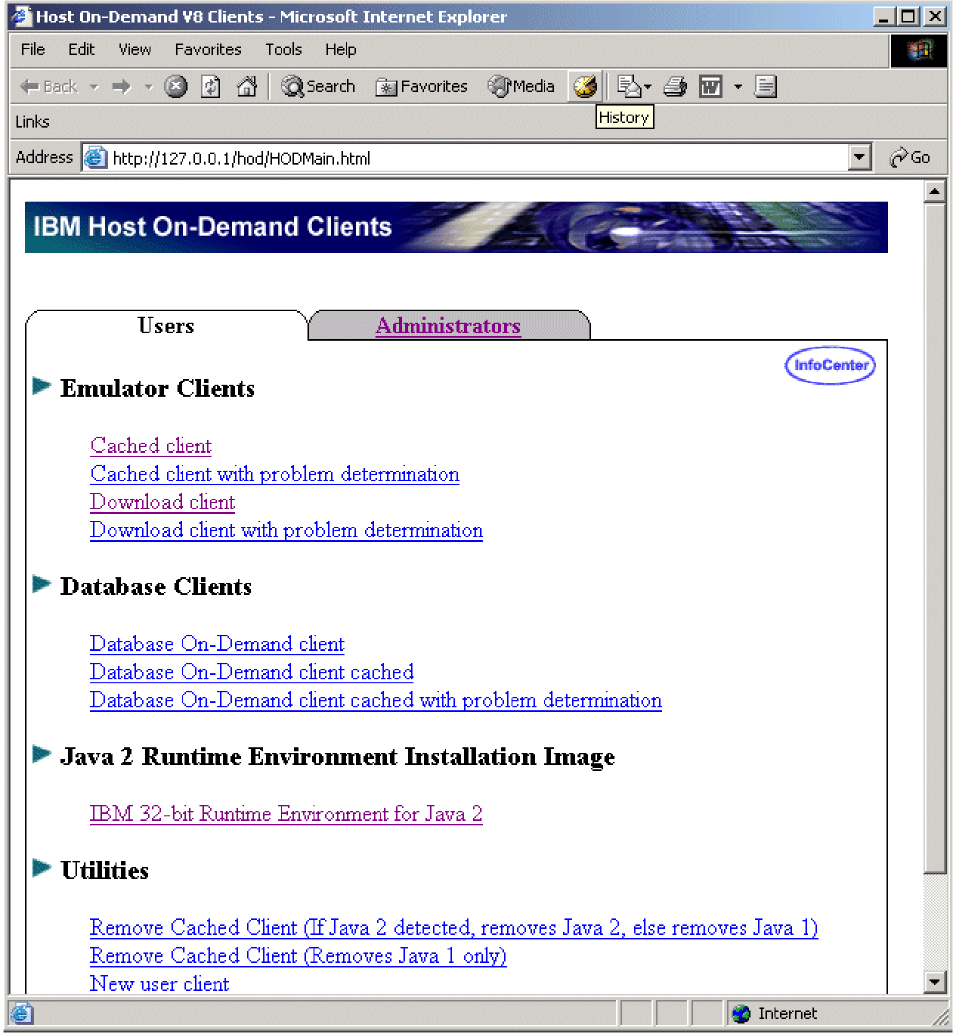
Host On-Demand provides a variety of types of clients: emulator clients, FTP clients, CICS Gateway clients, and database clients. Most of these are available as either a cached client or a download client.

This chapter introduces the various Host On-Demand clients and describes how you can use and customize them.

In addition, this chapter also discusses support for clients running on Java 2 enabled browsers.

5.1 Host On-Demand default clients

The following figure shows the default clients supplied with Host On-Demand.



http://127.0.0.1/hod/HODMain.html

IBM Host On-Demand Clients

Users | Administrators

Emulator Clients

- Cached client
- Cached client with problem determination
- Download client
- Download client with problem determination

Database Clients

- Database On-Demand client
- Database On-Demand client cached
- Database On-Demand client cached with problem determination

Java 2 Runtime Environment Installation Image

- IBM 32-bit Runtime Environment for Java 2

Utilities

- Remove Cached Client (If Java 2 detected, removes Java 2, else removes Java 1)
- Remove Cached Client (Removes Java 1 only)
- New user client

Figure 5-1 /hod/hodmain.html

The following table lists the Host On-Demand default clients. These clients use the Configuration server-based model. The Deployment Wizard may be used to create HTML files with custom versions of the emulator clients. See Chapter 14, “Deployment Wizard” on page 517 for details.

Table 5-1 Host On-Demand clients

Package	Client	HTML File
Administration clients	Administration client download	`HODAdmin.html`
	Administration client cached	`HODAdminCached.html`
	Administration client cached with problem determination	`HODAdminCachedDebug.html`
	Administration client with Start Session enabled	`HODAdminFull.html`
	Administration client cached with Start Session enabled	`HODAdminCachedFull.html`
	Administration client cached with problem determination with Start Session enabled	`HODAdminCachedDebugFull.html`
Emulator clients	Cached client	`HODCached.html`
	Cached client with problem determination	`HODCachedDebug.html`
	Download client	`HOD.html`
	Download client with problem determination	`HODDebug.html`
Database clients	Database On-Demand client	`HODDatabase.html`
	Database On-Demand client cached	`HODDatabaseCached.html`
	Database On-Demand client cached with problem determination	`HODDatabaseCachedDebug.html`
Utilities	Remove cached client (If Java 2 detected, removes Java 2, else removes Java 1)	`HODRemove.html`
	Remove cached client (Java 1 only)	`HODRemove.html?JavaType=java1`
	New user client	`NewUser.html`
	New user client cached	`NewUserCached.html`
	New user client cached with problem determination	`NewUserCachedDebug.html`

5.1.1 Administration clients

The administration client (`HODAdmin.html`) starts the Administration window where you can:

- Manage users, groups, and sessions
- Configure, manage and trace the Redirector service
- Configure Database On-Demand
- Enable security
- View trace and message logs
- Disable functions to end users

Refer to Chapter 7, “Administration” on page 265 for complete details on the functions and operations of the administration client. You must use one of the following clients to do administration. The Deployment Wizard does not have the capability to create customized administration pages.

Administration client cached

This client starts the administration client in a cached environment. Load this client if you want to use the administration client in a cached environment without problem determination. The advantage of the administration client cached is that it can be cached along with other cached clients in the browser. In releases prior to Version 5, the cached client had to be removed before the administration client could be loaded.

If you want to bookmark the administrator client cached, you must manually create the bookmark. It must point to `HODAdminCached.html`, so that Host On-Demand can compare the cached version to the server version. This allows Host On-Demand to recognize and notify you that a newer version of the administration client cached is available at the server.

Administration client cached with problem determination

This client also starts the administration client in a cached environment. Load this client if you need to use the administration client in a cached environment with problem determination (session logging and tracing).

Administration client with Start Session enabled

This client loads the download version of the full Administration client. The full administration client gives the administrator the additional ability of starting sessions to configure runtime properties. However, the download size of the full administration client is larger than the download size of the administration client.

Administration client cached with Start Session enabled

This client loads the cached version of the full Administration client. Like the cached version of the regular Administration client, this client can be cached along with the cached client in the browser.

Administration client cached with problem determination and Start Session enabled

Loads the cached version of the full Administration client with problem determination (session logging and tracing) enabled.

5.1.2 Download clients

A download client is one where the code is downloaded from the server on every invocation of the client. The advantage of the download client is that the browser does not need to be stopped and then restarted.

This client can be used when:

- You do not want to take up disk space on client machines by installing the cached client.
- The download time is not an issue.

> **Important:** Running a download client with a cached client loaded in the browser will result in inaccurate and unpredictable results. You must first remove a cached client from the browser before using a download client. See 5.5.2, “Remove cached client” on page 166 for more information.

For information on the Java 2 download client, see “The Java 2 download client” on page 212.

5.1.3 Cached clients

A Host On-Demand cached client has all the functionality of the download client. It is cached on your local disk the first time you download it. The next time you start the emulator session, only a small applet downloads from the server, reducing the time needed to start the session. When using a Java 1 or Java 2 enabled browser, the applet that is downloaded checks to see if the software on the server is more recent than the software that has been cached, and if so, the cached software is updated.

For more information about the Java 2 cached client, see “The Java 2 cached client” on page 203.

Beginning with Host On-Demand Version 5, all clients consist of a collection of smaller JAR/CAB files called components to allow for the administrator to create smaller clients, and to provide the ability to update individual components rather than the entire client. This has been called *componentization* and is more fully documented in 5.3, “Componentization” on page 163.

Since the clients are broken into components, only the specific component will be updated, and then only after that component has been referenced. Under most circumstances, you can continue to use the current level of the cached client to connect to a host while the newer components are downloading. See 5.4, “Smart caching” on page 164 for further information.

The cached client is persistent across operating system restarts and browser reloads. If you want to remove it, you must load `HODRemove.html`. See 5.5.2, “Remove cached client” on page 166.

Restricted users on Windows XP and Windows 2000

Restricted users of Windows 2000 and Windows XP can now install and use the Java 1 or Java 2 Host On-Demand cached client. A separate version of the cached client will be installed for each restricted user.

Previously, only users with administrator or power user authority could install and use the cached client on Windows 2000 and Windows XP.

Sharing the cached client on the Windows platform

The following sections discuss sharing the various clients on the Windows platform.

Sharing the Host On-Demand Java 2 cached client

On a multi-user Windows machine running either Windows 2000 or Windows XP operating systems, and either of the following two browser/Java combinations listed below, users can download their own independent version of the cached client:

- Internet Explorer and the Microsoft JVM (Java 1)
- Any supported browser with a Java 2 plug-in

If the JavaScript API is enabled, the cached client cannot be shared for Netscape and Mozilla Java 2 browsers due to a technical limitation.

Alternatively, you can add the following parameters using the HTML parameters selection of the Advanced Options window of the Deployment Wizard:

- ShareCachedClient

  Allows users to share a single instance of the cached client

- SharedCachedDirectory

  Allows you to specify the directory location where the cached client is to be installed

When the cached client is shared, but you do not specify a directory, the cached client is installed in the default directory:

```
\Documents and Settings\All Users\IBMHOD
```

If you specify a directory, for example `SharedCachedDirectory=c:\ibm,` the Host On-Demand cached client appends `IBMHOD\HODCC` to this string, and the cached client is installed in this new location, for example, `c:\ibm\IBMHOD\HODCC`. An administrator or power user must either create the install directory manually, or perform the first install of the shared cached client. In either case, the administrator or power user must change the security settings for this directory so that restricted users have read, modify, and write access. The administrator can either change the security settings and then download the cached client to the directory, or download the shared cached client to the directory and then change the security settings. If the security settings are not updated and a restricted user attempts to install the shared cached client, the user receives an error message that indicates there may be a problem with the file system, and the restricted user will not be able to use or update the cached client.

Once the administrator or power user changes the security settings, a restricted user can log on to Windows and can either install the shared cached client, or use (or update) a previously installed version of the shared cached client. Other restricted users can log on to Windows and use the cached client without having to download it from the Host On-Demand server again. They can also upgrade the shared cached client, if necessary. For Internet Explorer using the Microsoft JVM (Java 1), after the shared cached client is installed, any user that logs on to Windows to access the cached client for the very first time will need to restart the browser one extra time when prompted. If you do not want restricted users to share the cached client, a separate instance of the cached client is downloaded to the user directory for each restricted user.

If an administrator or a power user downloads the previous version of the cached client, and you want to allow restricted users to access it, the administrator or a power user must use `HODRemove.html` to remove the previous version of the cached client, and then change the security settings to the shared cached client directory to read, modify, and write for restricted users, as described above.

For information about removing a shared cached client, see “Removing a cached client shared by multiple users” on page 212. For information about the new cache design for Java 2 cached clients, see 5.18.1, “More information on the new Java 2 cache” on page 227.

Sharing the Host On-Demand Java 1 cached client

Multiple users on Windows XP, Windows 2000, Windows ME, Windows NT, or Windows 95/98 can share a single Java 1 cached client installation.

For users to share a single cached client installation, the system administrator must take the following steps:

1. Use the **Additional Parameters** tab of the Advanced options panel of the Deployment Wizard to add the ShareCachedClient parameter to the cached client HTML file.

   This step is required if some of the machines on which the cached client installation will be shared are running Windows 2000 or Windows XP.

   This step is not required if all the machines on which the cached client installation will be shared are running Windows NT, Windows Me, or Windows 95/98.

2. Modify each client machine to include the IBMHOD directory:

   a. On client machines running Windows 2000, Window XP, or Windows NT, have a user with administrator or power user status take the following steps:

      i. Create a directory named IBMHOD under the system `all users` directory. For example, if Windows 2000 is installed on the C: drive, the directory path is:

         `c:\Documents and Settings\All Users\IBMHOD`

      ii. Change the security settings for the IBMHOD directory so that restricted users have read, write, and modify access.

          If this step is omitted then a restricted user attempting to install or use a shared cached client will not be able to do so. Instead, an error message will be displayed indicating that there may be a problem with the file system.

      iii. If the IBMHOD directory already exists, run **`HODRemove.html`** to remove the previous version of the cached client.

      > **Note:** A user with administrator or power user status can create the IBMHOD directory automatically merely by installing the cached client. However, the user with administrator or power user status must still change the security settings of the IBMHOD directory as described above.

   b. On client machines running Windows ME or Windows 95/98, have any user create the following path:

```
c:\Documents and Settings\All Users\IBMHOD
```

After the above setup, any user can:

- Install the shared cached client
- Use the shared cached client
- Upgrade the shared cached client

After the shared cached client is installed, any user attempting to use the shared cached client for the first time will be prompted to restart the browser.

Java 1 cached client support across the Internet

If you deploy the Java 1 cached client to the Internet, consider that your users might use Host On-Demand with other business partners running Host On-Demand servers at different service levels. This could be a problem if your user needs different functions when accessing servers at different service levels. Components of different service levels are not supported within a single cached client, and there can be only one cached client on a machine. This section discusses the problems that might occur.

If you want your users to be able to attach across the Internet to servers running different versions of Host On-Demand, and you want your users to be able to run the cached client with these servers, then you must install Host On-Demand version 5.0.4 or higher on each server.

> **Note:** These problems do not occur with the Java 2 cached client. See 5.14.6, "Increased flexibility with Java 2 cached clients" on page 209.

The remainder of this subsection is applicable only to the Java 1 cached client, not to the Java 2 cached client.

Installed Java 1 cached client version is later than HOD server

If the software on the server is an earlier version than the cached software, the cached client applet checks the version levels of the components and prevents caching of any new components. To cache new components, remove the more recent version of the cached client, and then install the earlier version of the cached client. To avoid this problem, select all the functions the user needs (across all sites the user accesses) in the preload list when you create the HTML page using the Deployment Wizard.

Installed Java 1 cached client version is earlier than HOD server

When a client points to a server running a later version of Host On-Demand, and the upgrade test passes, all cached components are automatically upgraded (not only the components defined in the HTML page's preload list). Because all cached and new components are upgraded simultaneously, the upgrade might generate additional Web server load. After the upgrade, the client can point back to the server running the earlier version of Host On-Demand, and the later version of the cached client will function correctly.

Workarounds with Java 1 cached client

To prevent these complications with Java 1 cached clients, you can do some or all of the following:

- Select all the functions a user needs (across all sites the user accesses) in a preload list when you create an HTML page using the Deployment Wizard.
- Use the disable function of the Deployment Wizard to disable all functions not in the preload list, and the functions that are not needed for your users.
- Create separate HTML pages for different user groups.
- Give your HTML pages a name that identifies your company.

  If you are using locally stored preferences, the custom HTML pages you create *must* have names unique to your company, because the HTML file names are used to differentiate between the locally stored preferences of different sites. Using generic names could cause preference conflicts for your users.

If you have problems managing a cached client deployment across the Internet, see the Host On-Demand support Web site for more information:

`http://www.ibm.com/software/webservers/hostondemand`

5.1.4 Emulator clients

The emulator clients provide emulation support for:

- 3270 displays
- 3270 printers
- 5250 displays
- 5250 printers
- VT displays
- FTP clients

These are the most used clients. The emulator clients listed in Table 5-1 on page 151 provide support for all of these terminal emulators. The Deployment Wizard, (see Chapter 14, “Deployment Wizard” on page 517) provides you with the capability of custom creating an emulator client that supports one or more of these device types.

5.1.5 Problem determination clients

Problem determination clients have special functions that allow them to trace sessions and log information for problem determination purposes. The default Host On-Demand problem determination clients have the character string `Debug` appended to the name of the file, for example `HODDebug.html`. The Deployment Wizard can also create debug clients; however, the name of the file will not indicate that debugging components have been included.

5.2 Mac OS X clients

In this section, we will discuss Mac OS X clients and support issues.

5.2.1 Overview of Mac OS X support

In Host On-Demand V8, Mac OS X was added to the list of supported client OS. Supported browsers include Microsoft Internet Explorer and Safari.

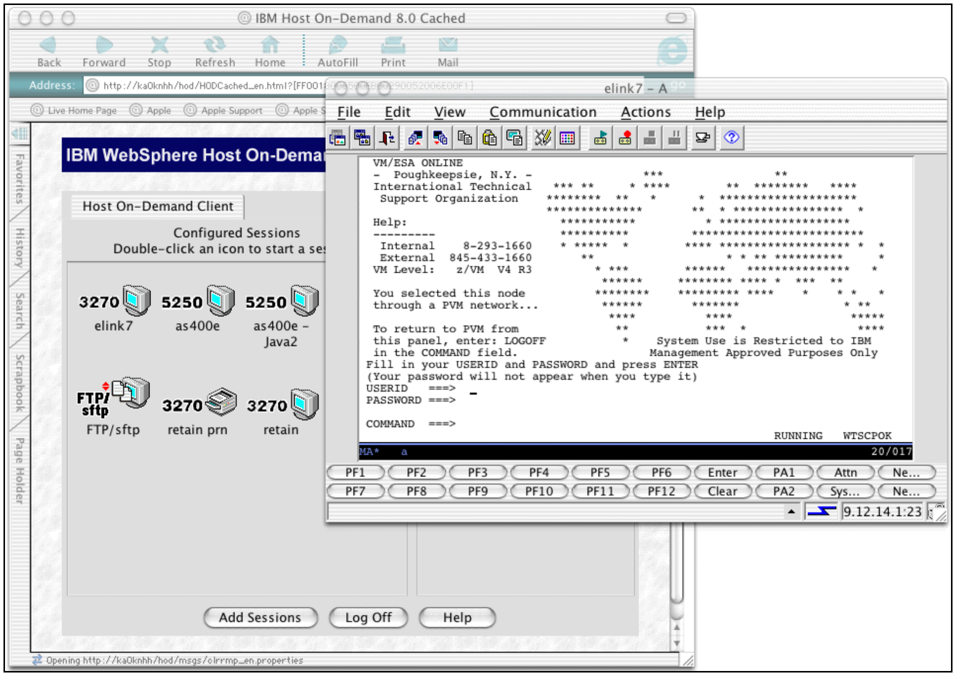
Safari is the Mac OS X default browser, which you can obtain from the following URL:

http://www.apple.com/safari/download/

You can also obtain Internet Explorer for Mac OS X from following URL:

http://www.microsoft.com/mac/

Only Java 2 clients are supported. There is no support for Java 1 clients, or Administration clients.



```
  VM/ESA ONLINE
  -  Poughkeepsie, N.Y. -
  International Technical
   Support Organization

  Help:
  ---------
   Internal    8-293-1660
   External  845-433-1660
  VM Level:   z/VM  V4 R3

  You selected this node
  through a PVM network...

  To return to PVM from
  this panel, enter: LOGOFF          System Use is Restricted to IBM
  in the COMMAND field.             Management Approved Purposes Only
 Fill in your USERID and PASSWORD and press ENTER
 (Your password will not appear when you type it)
 USERID   ===>  _
 PASSWORD ===>

 COMMAND  ===>
                                                          RUNNING   WTSCPOK
MA*   a                                                              20/017
```

Figure 5-2   Original Host On-Demand client on Mac OS X

5.2.2 Planning for Mac OS clients

Host On-Demand supports download clients, cached clients, and database clients on Mac OS X.

Supported browsers for Mac OS clients are listed as follows:

- Microsoft Internet Explorer V5.2 with JRE 1.3.1
- Safari V1 with JRE 1.3.1 or 1.4.1 (Mac OS X comes with JRE 1.3.1, but we recommend upgrading it to JRE 1.4.1).

There is no support for Netscape on Mac OS X.

You can download JRE 1.4.1 for Mac OS X from:
`http://www.applecom/`

Limitations:

The following limitations apply to Cached clients on Mac OS X:

- Available only for Java 2 clients, and there is no support for Java 1 clients
- No support on Host On-Demand administrator clients

- It is no use to preload cached clients from a CD or LAN drive. When the browser is redirected to the real Host On-Demand server, the plug-in considers that to be a distinct Host On-Demand server, and the client is cached again.
- On Mac OS X, you cannot install additional components after the initial download. You should take this into consideration when you are reducing the size of components using Deployment Wizard.
- The Host On-Demand Java files used to run the Host On-Demand cached client on a Java 2-enabled Web browser are stored in the Java Runtime Environment (JRE) cache. To remove the cached client on Mac OS X, you must use the Java control panel to clear the JRE cache.
- The options you can set to control upgrades with Deployment Wizard are not available on Mac OS X.
- The Java 2 cached client improvements covered later in this book do not apply to the Mac OS X Java 2 cached client. For details of each feature, please refer to 5.9.3, “Improvements to the cached client for Java 2” on page 181.

> **Note:** Because of the difference between Mac OS X and other operating systems, there are certain workarounds that users will have to make.
>
> For example, the mouse used for Mac OS has no right mouse button. In this case, in order to display context menus such as session properties, you will need to click the session icon while pressing down the Ctrl key. One thing that administrators and users need to be careful of is when you need to perform a right-click while a session is running. In this case, pressing the Ctrl key is also sent to the session, which may cause unpredictable results.
>
> A potential workaround is to unassign the Ctrl key using keyboard remapping.

5.2.3 Scenario using a Mac OS X client

In this section, we will discuss some tips for using Mac OS X as a Host On-Demand client.

Displaying Java Console

To display Java Console, you will need to activate it from the Java Plug-in control panel. You can also turn off the Java Console. The Java Plug-in control panel can be launched from following:

Machintosh HD -> Applications -> Utilities -> Java -> Java Plugin Settings (**Java 1.4.1 Plugin Settings** for JRE 1.4.1).

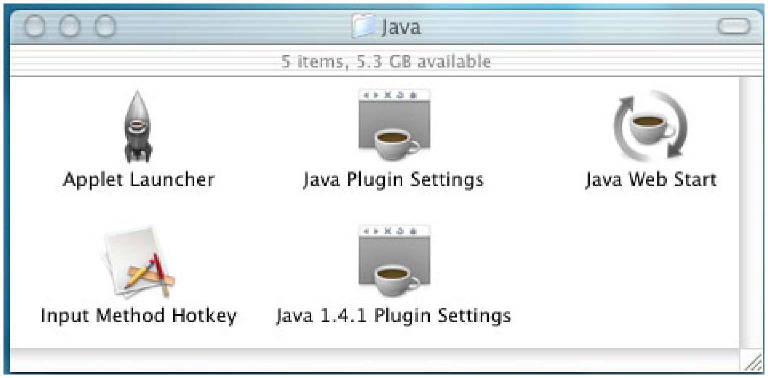
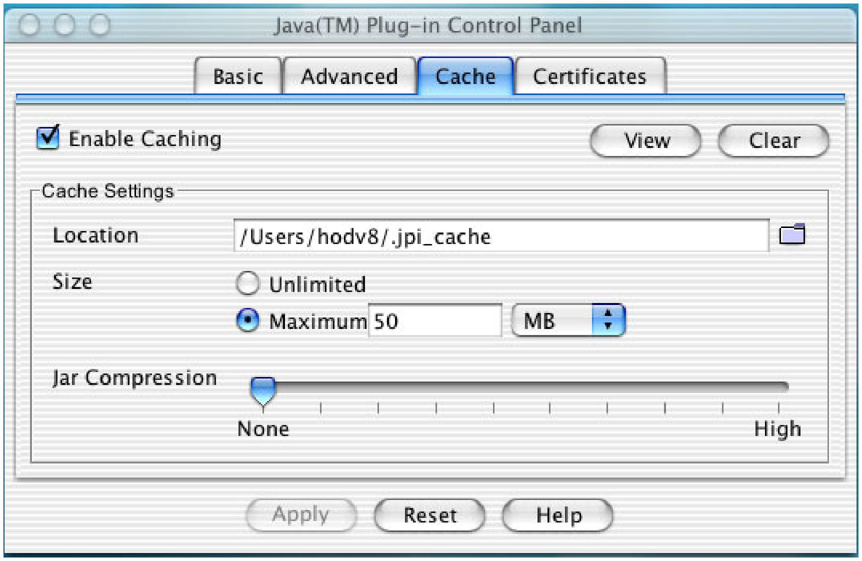


Figure 5-3 Launching Java Plug-in control panel

Removing cache

Since HODRemove.html is not supported to remove the Java-applet cache for Mac OS X, you must remove the cache using the Java Plug-in control panel.

1. Start **Java Plug-in Control Panel.**
2. Go to **Cache** tab.
3. Click **View.**
4. Choose files you want to remove, and click **Remove.**



☑ Enable Caching

Location /Users/hodv8/.jpi_cache

Size ○ Unlimited
● Maximum 50 MB

Jar Compression None

Figure 5-4 Removing cache from Java control panel

Access Web start client

The Web Start client is supported on Mac OS, which is similar to those on Windows. You can access Web Start control panel from following:

Macintosh HD -> Applications -> Utilities -> Java -> Java Web Start

For more information, refer to Chapter 16, “Web Start” on page 591.

5.3 Componentization

The Host On-Demand cached client has been identified as the overwhelmingly preferred Host On-Demand client. In Host On-Demand Version 4, the cached client needed to include all the class files that could possibly be used by all four emulator types and all functional components, such as macro recording and playback, ColorRemap, and all possible code pages. This produced a very large archive file of class files, many of which would probably never be used. Downloading these files, although done only when the files changed, created a response time problem for users on slower speed lines as well as a network utilization problem.

The cleanest way to resolve these concerns is to break each function into its own archive file, and then a smaller client could be built that contained only the functions required by the user. This technique is referred to as *componentization*.

With the introduction of componentization, Host On-Demand was able to implement smart caching. See 5.4, “Smart caching” on page 164.

Table 5-2 provides a breakdown of JAR/CAB files that are sent to the workstation for a cached client installation. In this table, the base install is represented by the first five JAR files (CAB files if using Internet Explorer). These files are common across all client emulators, and represent the minimum cache install available.

The lower portion of Table 5-2 includes files that are required for specific emulation requirements such as 3270 Display. By selecting a specific column, such as **3270 Display**, a list of required files may be obtained. The administrator can calculate the approximate size of the cached client and estimate installation time for a new installation or code update.

Table 5-2 Required class files by client

Class file names	3270 Display	5250 Display	3287 Printer	5250 Printer	VT100/ 220 Display	CICS Gateway
ha_en.jar	X	X	X	X	X	X
habasen.jar	X	X	X	X	X	X
hacp.jar	X	X	X	X	X	X
hodbasen.jar	X	X	X	X	X	X
hodimg.jar						
ha3270n.jar	X		X			
hafntap.jar	X	X				
hafntib.jar	X	X				
ha5250n.jar		X				
haprintn.jar			X	X	X	
havtn.jar					X	
hacicsn.jar						X
ha3270pn.jar			X			
ha5250n.jar				X		
ha5250pn.jar				X		
For further information, please refer to the IBM Host Access Toolkit documentation.						

5.4 Smart caching

Smart caching is the ability to cache and upgrade individual components of the client, even components that were not included in the initial loading of the client. A side benefit is the ability to create a smaller client footprint for network distribution, which includes only basic functionality for downloading to the workstation, and incrementally adding only those functions that the user actually uses rather than all the functions that the user may use. In Table 5-2 on page 164, you can see the basic components that are required to have a functional Host On-Demand client. The remainder of the associated JAR/CAB files are downloaded and maintained in permanent cache only when the user requests a function requiring that function, for example, a file transfer.

This configuration or packaging of required components is accomplished with the use of the Deployment Wizard. Refer to Chapter 14, “Deployment Wizard” on page 517 for details. Several independent configurations can be created to satisfy specific client requirements within a large diverse environment. For example, several organizations require keyboard remapping and file transfer capabilities. Instead of shipping the necessary JAR file to everyone, a specific HTML page is created for their unique requirements reducing the installation time and network contention. Other advantages include controlling specific configuration of the client’s capabilities. This may be necessary if the workstation is a shared device or security may be an issue.

5.5 Utility clients

There are three valuable utility clients:

- New user client

  This client allows non-administrative users to create other user accounts.

- Remove cached client (autodetect Java 1 or Java 2)

  This client is used to remove a Java 1 or Java 2 cached client from a browser.

- Remove cached client (Java 1 only)

  This client is used to remove a Java 1 cached client from a browser.

5.5.1 New user client

If the administrator has checked the **Allow users to create accounts** option in the Users/Groups view of the Host On-Demand administration applet, users will be allowed to load a special client, `NewUser.html`, which allows them to create accounts for themselves or other users. The purpose of this client facility is to remove some of the load from the administrator and delegate the responsibility for creating users to department managers, site managers, or other designated people.

The default HTML file will insert users into the default Host On-Demand group, `HOD`, when an account is created. This file can be used as a template to create customized applets that will allow a user to be inserted into specific groups or combinations.

To add users to a group other than `HOD`, you must modify the following HTML parameter:

```
<PARAM NAME="Groups" VALUE="HOD">
```

You may replace HOD with any previously defined group. If you are using the Host On-Demand default data store, you may specify more than one group separated by commas. For example, by specifying the following parameter:

```
<PARAM NAME="Groups" VALUE="ProjectLeader, HOD">
```

Users will be added to both the ProjectLeader and HOD groups.

This utility is available in three forms:

- Download client - NewUser.html
- Cached client - NewUserCached.html
- Cached problem determination - NewUserCachedDebug.html

5.5.2 Remove cached client

HODRemove.html is the remove-cached client utility. In Host On-Demand Version 4 this utility was used to remove the cached from the Netscape browser after Host On-Demand stopped using Netscape's smartupdate function to manage the persistently cached applications. Users of Internet Explorer continued to use the facilities of Internet Explorer to remove the cached client. With the introduction of Host On-Demand Version 5 and componentization (see 5.3, "Componentization" on page 163), it became necessary for Host On-Demand to assume management of the cached clients directly. This required all browsers to use the HODRemove.html tool to clear the cache.

In Host On-Demand 8.0, the remove cached client function was divided into two types, both of which are handled by HODRemove.html:

1. Remove Cached Client (If Java 2 detected, removes Java 2, else removes Java 1)

   This selection causes HODRemove.html to check whether a Java 2 environment is installed, regardless of whether it is enabled or not. If yes, it tries to remove the Java 2 cached client, if no Java 2 is installed, it removes the Java 1 cached client if any is present.

2. Remove Cached Client (Java 1 only)

   This selection causes HODRemove.html to remove Java 1 cached client data, if any is present. (However, this selection does not work if the Web browser is Netscape 6.x.)

For more information see 5.14.7, "Removing the cached client" on page 209.

5.6 CICS Gateway client

The CICS Gateway client is a special 3270 emulator client. It connects only to a distributed CICS Transaction Gateway, thus forcing a three-tiered environment. The CICS Gateway client acts as a 3270 Telnet server, communicating with the client through TN3270 protocol, and with CICS through the SNA protocol.

There are several limitations to the CICS Gateway client that force most users to select the standard 3270 emulator client:

- SSL sessions are not supported.
- You cannot sign on to CICS.
- You are limited by the EPI subset (no BMS PAGING/ACCUM, no RETURN IMMEDIATE).
- No ATI support (STARTed transactions)
- The CICS Gateway client must connect through a distributed CICS Transaction Gateway, thus forcing a three-tiered environment and arbitrarily increasing path lengths.
- The CICS Gateway client included in Host On-Demand V8 requires CICS Transaction Gateway V5.0.1.

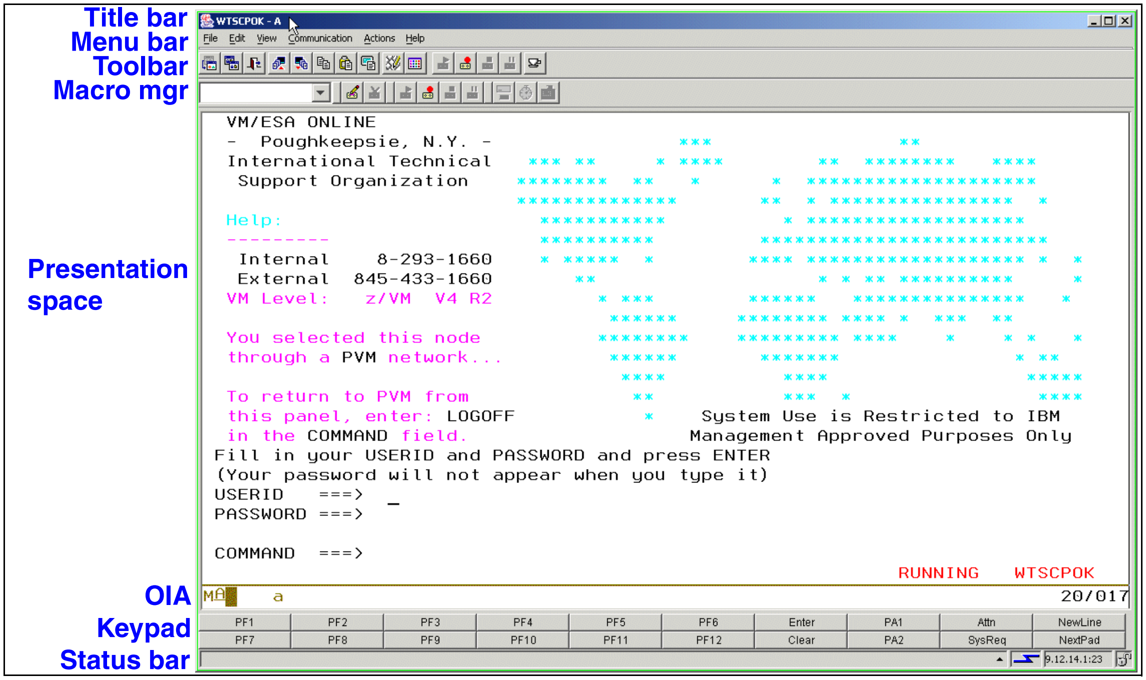
Because of the above limitations, we recommend that under normal circumstances you use the standard TN3270 emulator client.

5.7 Database On-Demand

Refer to Chapter 6, “Database On-Demand” on page 239 for details on the Database On-Demand client.

5.8 The emulator session window

An emulator session window consists of a title bar, a menu bar, a toolbar (with or without explanatory text), a presentation space, an operator information area (OIA), a keypad, and a status bar at the bottom of the window, as illustrated in Figure 5-5.



```
  VM/ESA ONLINE
  -  Poughkeepsie, N.Y. -
  International Technical
   Support Organization

  Help:
  ----------
   Internal     8-293-1660
   External   845-433-1660
  VM Level:    z/VM   V4 R2

  You selected this node
  through a PVM network...

  To return to PVM from
  this panel, enter: LOGOFF                        System Use is Restricted to IBM
  in the COMMAND field.                          Management Approved Purposes Only
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                              RUNNING    WTSCPOK
MA      a                                                                   20/017
```

Figure 5-5   Host On-Demand session

In this section we will describe the OIA, and then discuss how the user or administrator tailor an emulator session in the following ways:

- Customizing the toolbar
- Color remapping
- Keyboard remapping

5.8.1 Operator information area

The operator information area (OIA) is located across the bottom portion of the session window. This is where communication information is displayed. Almost every position in the area is used at some time, though many may be blank at any one time. The indicators are all explained in the Host On-Demand online help, but some deserve special mention:

- The first three columns show the type of connection and the condition of the host application. As you log on and move through an application, the indicator in column 3 changes.
- If the session is using SSL security and is connected in encrypted mode, column 4 has a + sign.
- Column 7 shows the session ID or short name from a to z.

- Starting in column 19, you will sometimes see a Communications or Program Check message, which includes a number. Such messages do not necessarily indicate a problem but merely the status of the connection. For example, you may see `COMM 657`, followed by `COMM 655` as the handshaking progresses and session connects; the length of time during which the messages appear depends on the performance of the various links and devices in the path.
- Column 75 through 80 indicate the position of the cursor by row and column. The position does not vary according to the screen size.

Table 5-3 Operator information area (OIA) fields

Column	Status character	Description
1	M	Indicates a connection has been established to a Telnet server
2	A	The protocol in use is TCP/IP.
3	* or p ?	- The session has established an LU-LU connection with an application program. - A SSCP-LU connection has been established but the connection has not been established to the application. -The session bind has not been established or is not connected.
4	+	When the session data is encrypted, the character “a” will change to “a+”.
7	a-z	Indicates which host session you are using.
9-17	X[] X SYSTEM X <-o->	- (3270 session only) System response time. It is made up of network hops and system response time until the keyboard is unlocked for additional input. - Application or transaction is in response mode. Keyboard is locked until process is complete. -Indicates that an attempt was made to insert a character into a protected field. Click **Reset** and move to an edit or update field.
19-26		
75-80		Cursor position

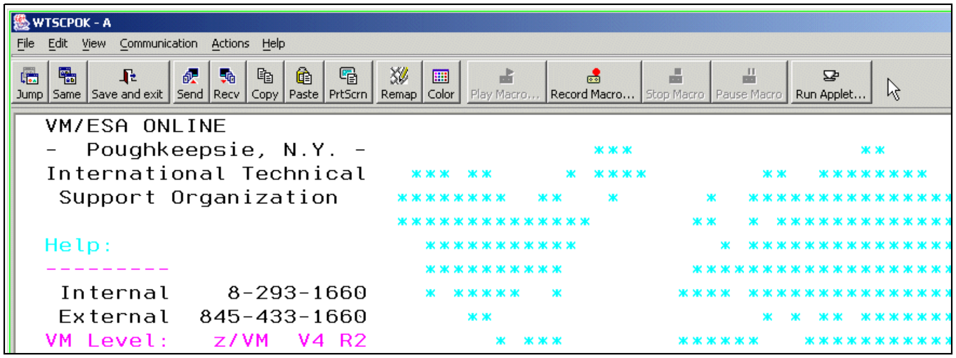
Color remapping of the OIA cannot be modified by using the mouse pointer and selecting an area. It requires the modification to be done by utilizing the Advanced color remapping window (see 5.8.3, “Color remapping” on page 174).

5.8.2 Customizing the toolbar

Toolbar customization allows administrators and users to add, edit, and remove buttons on the session toolbar. These buttons can be configured to launch an applet, run an application, go to a URL, run a macro, or perform a menu function. The toolbar settings are saved for future sessions.

Administrators can deploy their own customized toolbars either by customizing a session during the Deployment Wizard stage, or at a later stage by importing a customized session for a group or user in the administration utilities. By pre-customizing the toolbar, this feature can be disabled for the user so they cannot add, modify, remove, or reset the toolbar.

By default the toolbar appears with the following buttons; for clarity, the toolbar text has been enabled (see Figure 5-6).



```
VM/ESA ONLINE
-  Poughkeepsie, N.Y. -                ***                **
International Technical   *** **     * ****        **  ********
 Support Organization    ********  **   *      *  ***************
                         **************       **  * *************
Help:                      ***********          * ***************
---------                  **********         *******************
 Internal    8-293-1660    * *****  *        **** ***************
 External  845-433-1660       **                   * * ** *******
VM Level:   z/VM  V4 R2         * ***        ******   ***********
```

Figure 5-6 Default 3270 toolbar with toolbar text enabled

Add button

By right-clicking in the toolbar area and selecting **Add Button...** you will be presented with the window shown in Figure 5-7.

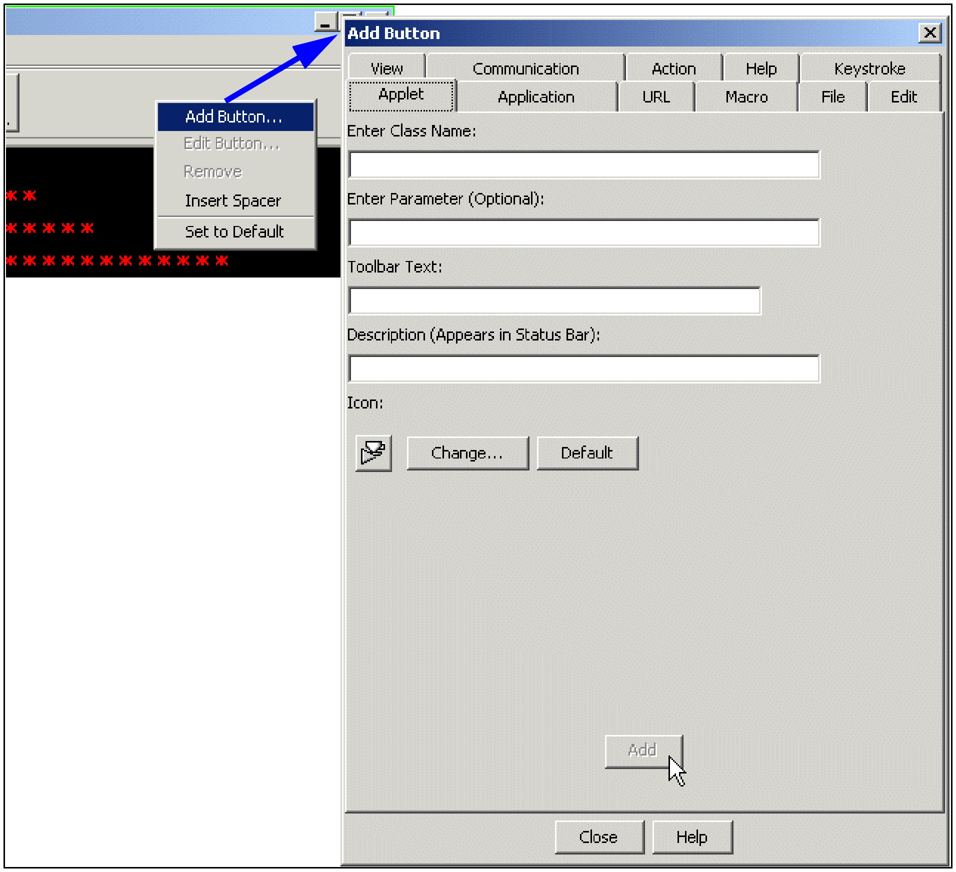


Figure 5-7 Add Button window for 3270 session

Each button type has a unique attribute, for example, the Class name for the applet, along with the two common fields, Toolbar, Text, and the Description. The Description will appear in the status bar at the bottom of the client window when the mouse passes over the button.

If a user has a disabled function such as playing a macro, they will not see that tab on the Add Button window.

The tabs are arranged in the following order:

- Applet

  This allows you to specify an applet you want to launch. Type the class name with or without an extension. The applet must implement the ECLAppletInterface in order to run.

- Application

Specify the full application path, along with any parameters in accordance with the platform syntax. A Browse feature is provided as an aid in locating the application.

- URL

  Enter the URL that will be opened in a browser window.

- Macro

  Choose from one of the prerecorded macros. The Toolbar Text and Description fields will default to the macro name. These default values can be edited if desired.

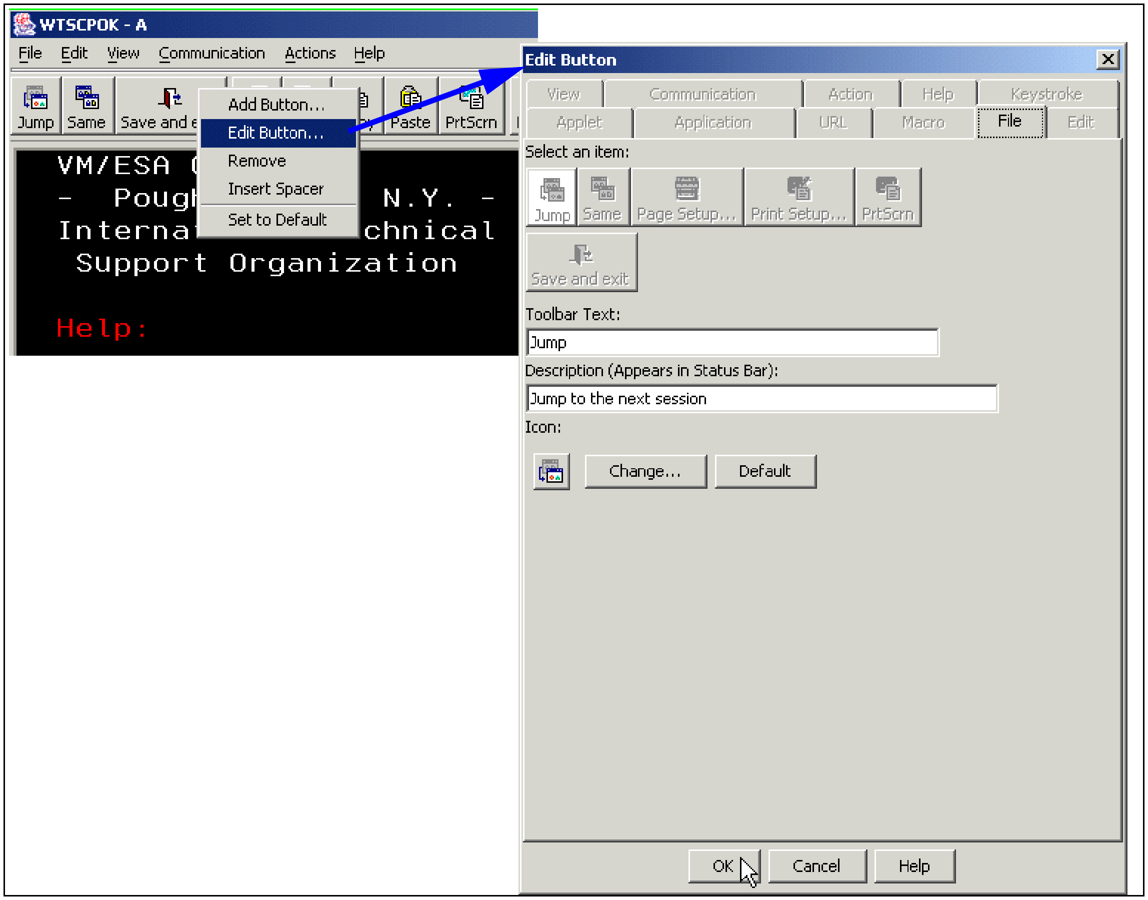
The File, Edit, View, Communication, Action, and Help tabs are associated with the drop-down menu functions.

The new button will appear to the left of where you right-clicked the toolbar. You can also add a button by selecting from the drop-down menu **Edit -> Preferences -> Toolbar -> Add Button....** When selecting from the drop-down menu, the new button will be added to the end of the toolbar.

Modifications to the existing toolbar buttons and layout can be achieved by right-clicking either the button to be modified, or elsewhere in the toolbar to insert spacers.

Edit button

By right-clicking the desired button, and choosing **Edit Button...,** an Edit window is displayed allowing you to modify the button attributes (Figure 5-8).



Toolbar Text: Jump

Description (Appears in Status Bar): Jump to the next session

Figure 5-8 Modifying existing toolbar buttons

Remove button

Removing a toolbar button is done by right-clicking the button, and selecting **Remove**.

Insert Spacer

Toolbar buttons can be grouped together or separated by the use of toolbar spacers. By right-clicking the toolbar and selecting **Insert Spacer**, a spacer is inserted to the left of where you clicked, with the outer buttons being shifted to the right.

Set to default

By selecting **Set to Default**, the toolbar customizations will be removed, and the toolbar will be reset back to the default settings. If a user resets a session that contains customizations defined by the administrator for a group, as well as personal customizations, both levels of customizations will be removed for the period of that login. The administrator-defined customization will return on the next login; however, the personal customization will have been permanently removed.

Customizing the toolbar for spawned clients will not be saved, for example, making a file transfer in the VT session brings up the FTP client. While it is possible to modify the toolbar for the spawned FTP client, the next invocation of this FTP client will show the default toolbar.

> **Note:** The Macro Manager toolbar item *cannot* be customized.

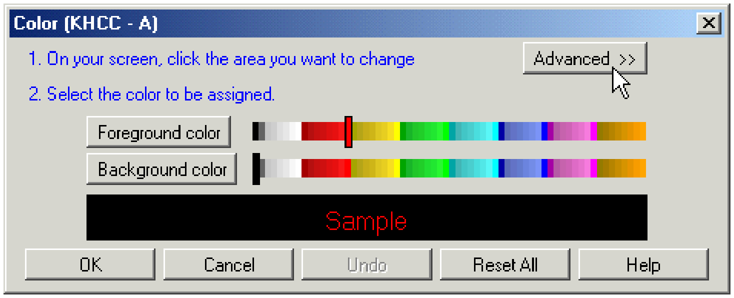
5.8.3 Color remapping

Each host screen is made up of fields with attributes and elements. Elements are simply a way to group fields that share the same attributes. When you remap a color, all the fields that share those same attributes throughout your host applications will also remap to the new color. If you are not familiar with field elements and attributes, you may be surprised to see that other fields throughout your host applications will be remapped to the same color. In addition, you may find other fields that were the original color will not be changed. These fields do not contain the same attributes, so there are different elements.

There are two ways to access the color mapping windows for Host On-Demand:

- From the drop-down menu, selecting **Edit -> Preferences -> Color...**
- Clicking the **Setup display color** button on the toolbar

The first window displayed is the basic color window (see Figure 5-9 on page 175). To change a screen element, you must first click it in the session window. The sample text will then adopt the attributes of this element. If the element has foreground or background colors, they can be modified by clicking the desired color in the palette. Foreground or background colors may also be specified using RGB values by clicking either the **Foreground color** or **Background color** buttons adjacent to the color palettes. In order to modify the OIA, you must use the Advanced window as described below.

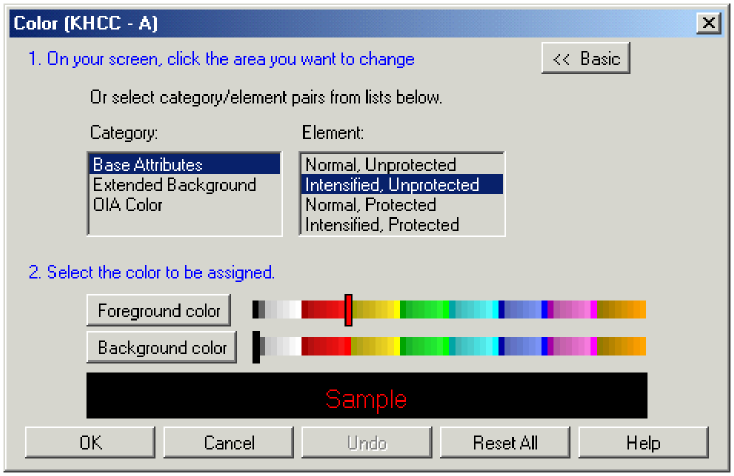

Color (KHCC - A)

1. On your screen, click the area you want to change

2. Select the color to be assigned.

Figure 5-9 Basic color mapping window

The Advanced color mapping window (see Figure 5-10), which is toggled by clicking **Advanced**, allows modification to the base attributes, extended background as well as the operator information area (OIA). Each session type, 3270, 5250, and VT, has its own unique elements that may be modified. These elements and attributes are listed within the Host On-Demand online help.


Color (KHCC - A)

1. On your screen, click the area you want to change

Or select category/element pairs from lists below.

Category:
- Base Attributes
- Extended Background
- OIA Color

Element:
- Normal, Unprotected
- Intensified, Unprotected
- Normal, Protected
- Intensified, Protected

2. Select the color to be assigned.

Figure 5-10 Advanced color mapping window

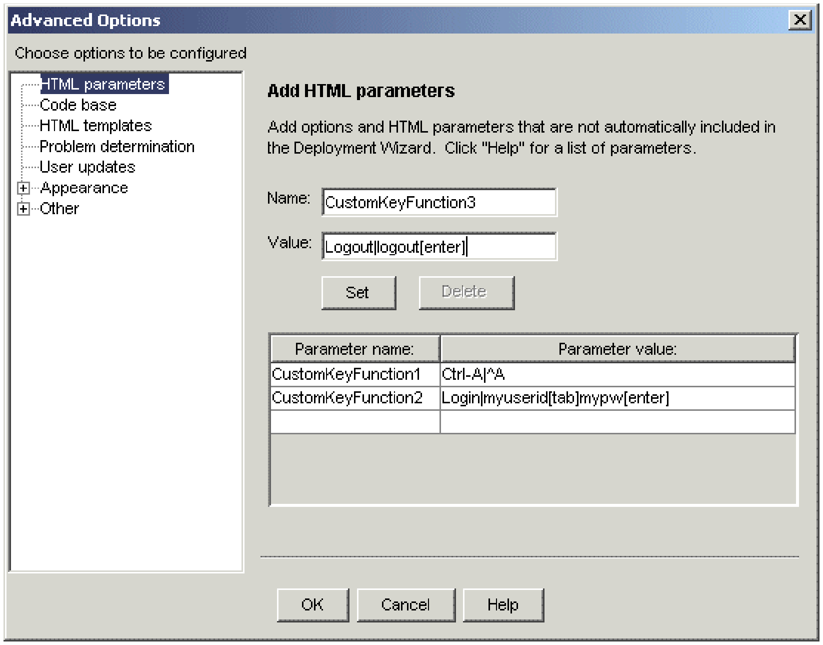
The Host On-Demand online documentation provides further information and procedures for modifying the host session colors.

5.8.4 Keyboard remapping

Most common host system functions are mapped to a key, but some are not. You may want to change the function of a key, map an undefined function, or create a new function that currently is not mapped. The keyboard remapping function provides the ability to display keyboard assignments on a per-key basis. The basic procedures are covered in the Host On-Demand online documentation; however, it may prove helpful to discuss assigning keys to custom functions.

Assigning keys to custom functions

If you want to assign a key or key combination to a custom function that is not listed under any categories in the Keyboard window, you must first define the functions by adding them through HTML parameters. For pages generated through the Deployment Wizard, the custom functions must be added using the Advanced Options window as shown in Figure 5-11.



Add options and HTML parameters that are not automatically included in the Deployment Wizard. Click "Help" for a list of parameters.

Name: CustomKeyFunction3

Value: Logout|logout[enter]

Parameter name:	Parameter value:
CustomKeyFunction1	Ctrl-A|^A
CustomKeyFunction2	Login|myuserid[tab]mypw[enter]

Figure 5-11 Creating custom functions in the Deployment Wizard

In the example, adding a log-off function requires the following:

Parameter name This must be CustomKeyFunction*X*,where *X* is the next ordinal number, in this example *3*.

Parameter value This is the combination of *Custom Function identified | function data*, for example, *Logoff|logoff[enter]*. Executing this function would be the equivalent of typing `logoff` followed by pressing the Enter key.

For HTML pages not generated through the Deployment Wizard, you add the parameter to the applet tag as highlighted in Example 5-1.

Example 5-1 Adding custom key functions to the applet tag

```
<applet archive=CachedAppletSupporter.jar mayscript name="CachedAppletLoader"
code="com.ibm.eNetwork.HOD.cached.appletloader.CachedAppletLoader" width="584"
height="450">
<param name=Cabinets     value=CachedAppletSupporter.cab>
<param name=BookmarkPage value=AutoHODCached.html>
<param name=CachedClient value=true>
<!-- put Host On-Demand applet parameters here -->
<param name=CustomKeyFunction1 value=Logoff|logoff[enter]>

<p>If you are reading this message, your client platform is not capable of
running
IBM Host On-Demand.  To run IBM Host On-Demand, you must have a Java-enabled
web
browser such as Netscape Navigator or Microsoft Internet Explorer.
</applet>
```

Note: Further information on coding the parameter value is included in the Host On-Demand online help.

After completing the session information in the Deployment Wizard, or having modified the HTML and refreshing the session in the browser, you will now see Custom Functions listed in the Category list box shown in Figure 5-12.

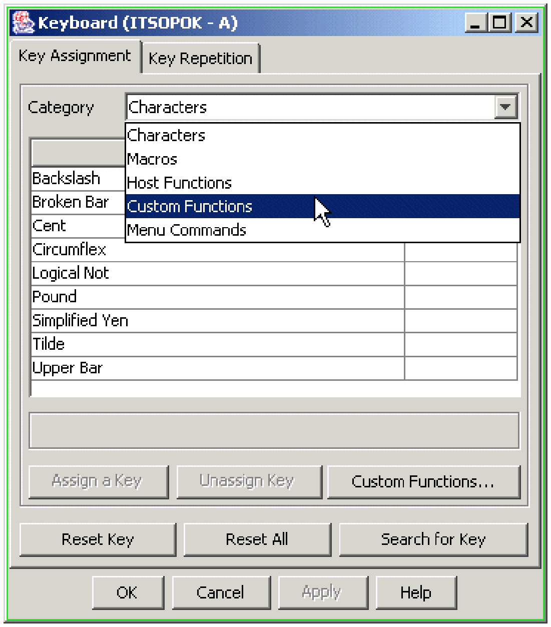
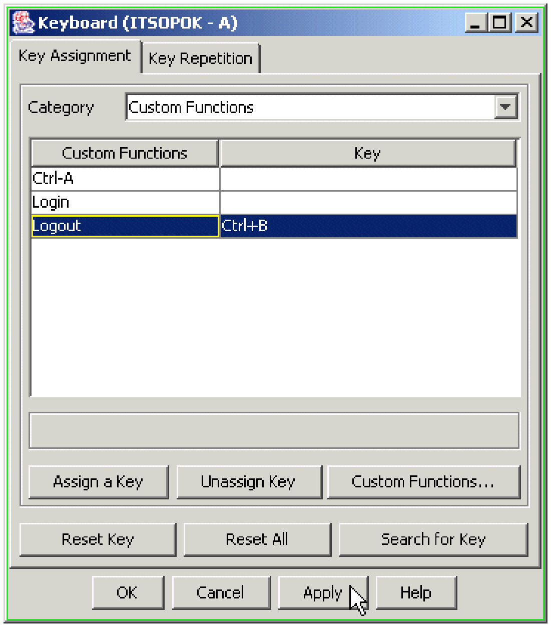


Figure 5-12 Custom Functions has been added to the category drop-down menu

Keys can now be assigned to the custom functions in the usual way, as shown in Figure 5-13.



Category: Custom Functions

Custom Functions	Key
Ctrl-A	
Login	
Logout	Ctrl+B

Figure 5-13 Mapping keyboard shortcuts to custom functions.

After this mapping has been saved, in this example, pressing Ctrl+B is the same as typing `logoff` and pressing the Enter key.

5.9 Java 2 support

There are several reasons why customers should consider making the transition from Java 1 browsers to Java 2-enabled browsers:

- Vendors who provide JVMs that use Java 1 are gradually withdrawing their support of these products. Withdrawing their support means no longer committing to fix bugs (including security bugs) or no longer making these products available.
- Java 2 is a proven technology and is actively supported by vendors.
- Java 2 provides capabilities that Java 1 lacks, including support for accessibility features.

Host On-Demand Version 8.0 continues to support both Java 1 and Java 2-enabled browsers. The Host On-Demand server has separate Java 1 and Java 2 versions of the Host On-Demand client. If a user is running a Java 1 browser and points to a Host On-Demand HTML page, then that user gets the Java 1 version of the Host On-Demand client. Likewise, if the user is running a Java 2-enabled browser and accesses a Host On-Demand HTML page, then that user (in most cases) gets the Java 2 version of the Host On-Demand client.

However, even though Host On-Demand has both a Java 1 and a Java 2 version of the client, the Java 2 version continues to acquire new features that the Java 1 version lacks, because the underlying Java 1 JVM does not contain the support required.

5.9.1 Features that take advantage of Java 2

The following features of Host On-Demand are available to a Host On-Demand client only if:

- The client is running a Java-2-enabled browser, and the client Java type of the HTML file has been set to `Java 2` or `Autodetect`.

The features are:

- Web Start client
- Support for the Secure Shell (SSH) for VT display sessions and secure file transfer protocol (SFTP) sessions.
- Accessibility features for persons with physical disabilities. These changes affect the runtime and the Deployment Wizard (requires Java version 1.4 or later).
- Auto Input Method Editor (IME) and On-the-Spot conversion for DBCS languages.

  Auto IME is the ability to switch between editing modes when moving from a DBCS field to a non-DBCS field or vice versa. On-the-spot conversion is the ability to select from among several closely related DBCS characters using a popup that appears in a location that is contiguous to the editing area.
- Print Screen Enhancements: Page header and footer, and the ability to set margins, orientation, paper size, and paper source.
- Internet Protocol Version 6 (IPv6)
- For bidirectional languages, support is now provided for OS/400 Coded Character Set Identifiers (CCSIDs) for displaying Unicode characters.

For additional information on these features, see the Host On-Demand online documentation.

5.9.2 Terms defined

Please note the terms below and their meanings in this redbook.

Table 5-4 Terms defined

Term:	**Meaning in this book:**
Java 1	Refers to a Java 1.1.x JVM
Java 2	Refers to a Java 1.3.x or Java 1.4.x JVM
Java 1 class file	A class file produced by a Java 1 compiler.
Java 2 class file	A class file produced by a Java 2 compiler.
Java 1 browser	Netscape 4.x, or Internet Explorer with only its built-in Java 1 JVM
Java 2 enabled browser	Netscape 6.x or Internet Explorer with the Java 2 plug-in installed.
Java 1 cached client, Java 1 download client	The version of Host On-Demand compiled with a Java 1 compiler, and intended to be run primarily on a Java 1 browser.
Java 2 cached client, Java 2 download client	The version of Host On-Demand compiled with a Java 2 compiler, and intended to be run on a Java 2 enabled browser.

5.9.3 Improvements to the cached client for Java 2

In version 7.0, Host On-Demand greatly expanded its Java 2 support and added new features that take advantage of Java 2 capabilities. With Host On-Demand Version 8, the Java 2 cached client was brought up to the same level of user-friendliness and flexibility as the Java 1 cached client. With the Java 2 cached client, you can now do the following:

- Install the Java 2 cached client from a LAN drive or CD drive.
- Share the Java 2 cached client between more than one user on Windows 2000 or Windows XP. For more information, refer to *Cached client support for Windows 2000,* and *Windows XP in Planning, Installing, and Configuring Host On-Demand.*
- Remove the Java 2 cached client in one operation, without clearing the Java 2 plug-in's cache. For more information, refer to 5.14.7, "Removing the cached client" on page 209.
- Upgrade the Java 2 cached client in the background.

Note: The following restrictions apply:

- Users upgrading the cached client from Host On-Demand 7 to Host On-Demand 8 cannot choose to upgrade in the background.
- A few Java 2 cached client types cannot be upgraded in the background. See *Improvement support limitations*.

Almost all Host On-Demand Java 2 cached clients support these improvements. The Java Web Start client also supports these improvements.

Improvement support limitations

The following types of Java 2 cached clients do not support the improvements to the Java 2 cached client:

- Java 2 Administration cached clients
- Java 2 cached clients on the Apple Mac OS X
- Java 2 emulator cached clients that have the JavaScript Session Manager API enabled

5.9.4 Look and feel with Java 2 version of Host On-Demand

This section describes some of visible differences between the Java 1 version and the Java 2 version of the Host On-Demand runtime.

If you are running an HTML file that was created or edited with the Host On-Demand 8.0 Deployment Wizard, and the HTML file's client Java type is Java 2, and you are not seeing the differences listed below, then try clearing the browser's cache and restarting the browser.

- The window containing the session icons on the Host On-Demand desktop has a tab labeled Host On-Demand Client. The tab is on the left side of the upper edge of the window. See the figure below.

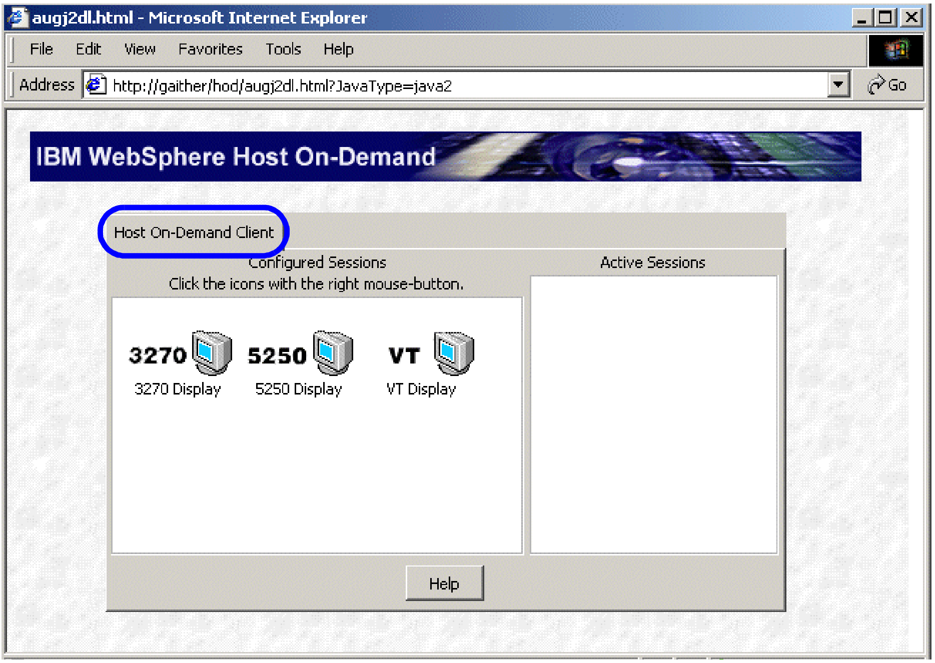
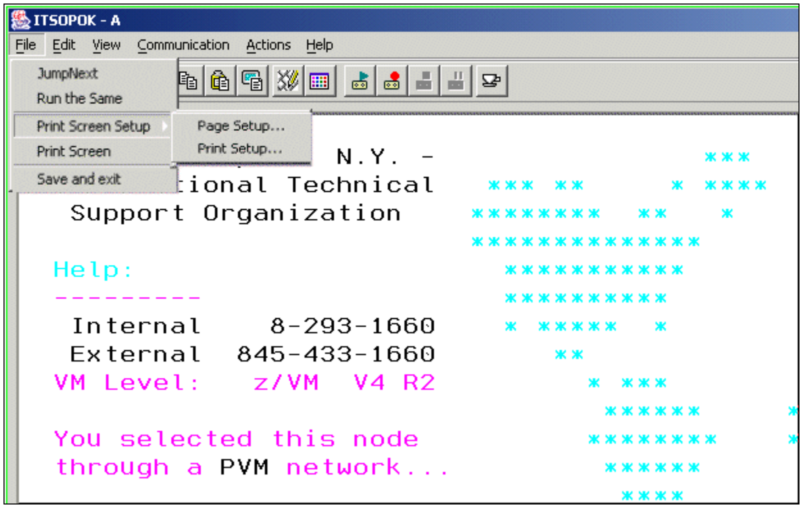

augj2dl.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://gaither/hod/augj2dl.html?JavaType=java2
Go
IBM WebSphere Host On-Demand
Host On-Demand Client
Configured Sessions
Click the icons with the right mouse-button.
Active Sessions
3270
3270 Display
5250
5250 Display
VT
VT Display
Help

Figure 5-14 Java 2 window containing session icons has tab

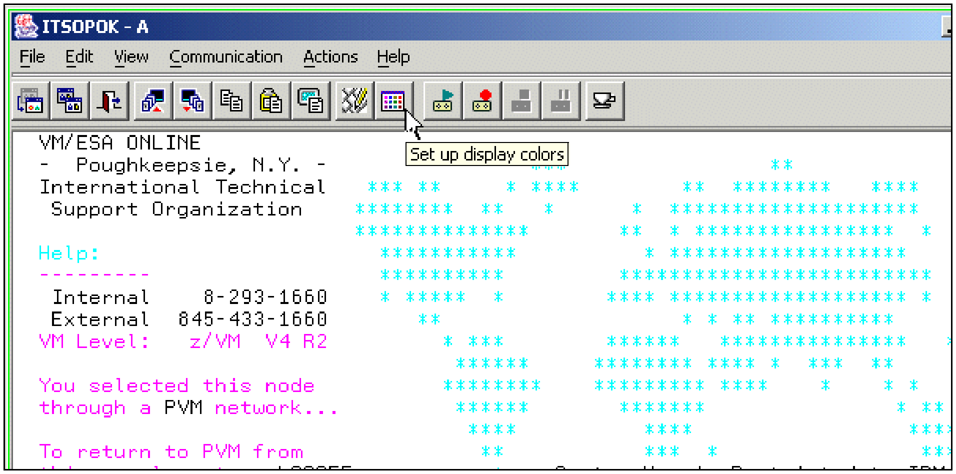
- After a session is started, clicking **File** on the session panel's menu bar pops up a submenu that includes the option Print Screen Setup. The figure below shows a session panel with the **Print Screen Setup** menu option selected.



```
                      N.Y. -
   tional Technical
 Support Organization

Help:
---------
 Internal     8-293-1660
 External   845-433-1660
VM Level:   z/VM  V4 R2

You selected this node
through a PVM network...
```

Figure 5-15 Java 2 session window with Print Screen Setup option

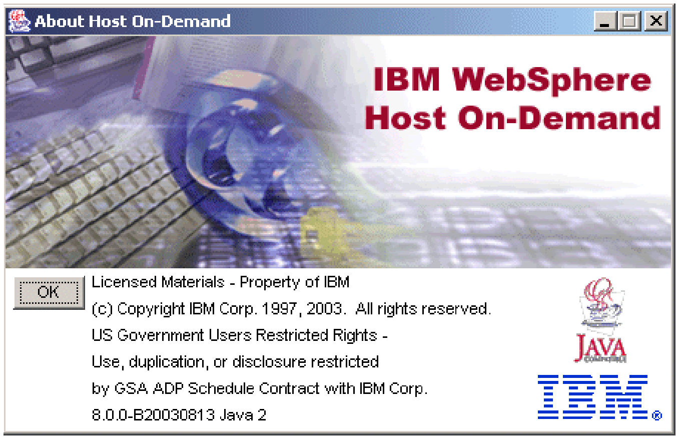
- After a session is started, moving the mouse pointer over a graphics image inside the session panel causes a small text popup to appear. This is an illustration of the capability of Java 2 to provide assistive information for computer users with physical handicaps. The figure below shows one of these pop-ups with the text: `Set up display colors`



```
VM/ESA ONLINE
-  Poughkeepsie, N.Y. -
International Technical
 Support Organization

Help:
---------
 Internal     8-293-1660
 External   845-433-1660
VM Level:    z/VM  V4 R2

You selected this node
through a PVM network...

To return to PVM from
```

Figure 5-16   Java 2 session window with text popup over graphic image

- The Host On-Demand version information on the session panel's About box includes the words Java 2. The figure below shows the About box. Note the words `Java 2` at the bottom of the box as part of the version information.

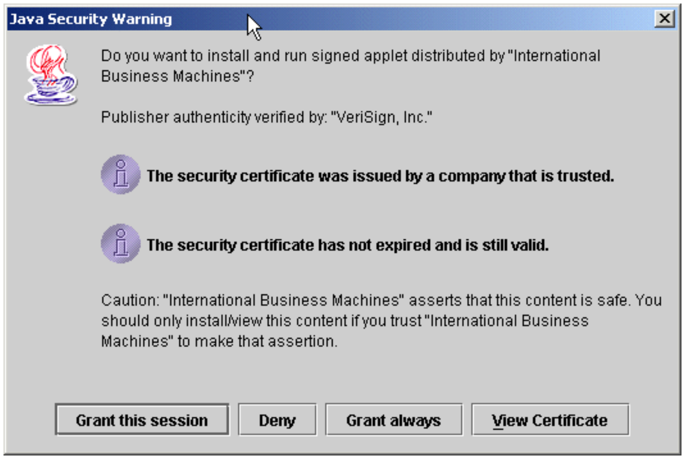


Licensed Materials - Property of IBM
(c) Copyright IBM Corp. 1997, 2003. All rights reserved.
US Government Users Restricted Rights -
Use, duplication, or disclosure restricted
by GSA ADP Schedule Contract with IBM Corp.
8.0.0-B20030813 Java 2

Figure 5-17   About box for Java 2 version of Host On-Demand

- The Java 2 Plug-in's Java console includes the same version information as the About box, including the words Java 2. See Figure 5-30 on page 220.
- Different Java security message box.

  The Java 2 security message box is different from the Java 1 security message box. Also, for Java 2 just one message box is popped up, and it is for all the privileges requested. In contrast, for Java 1 a separate message box is popped up at the time each type of privilege is requested. The figure below shows the Java 2 security message box for the IBM Java 2 Plug-in 1.3.1 for Win32.



Do you want to install and run signed applet distributed by "International Business Machines"?

Publisher authenticity verified by: "VeriSign, Inc."

The security certificate was issued by a company that is trusted.

The security certificate has not expired and is still valid.

Caution: "International Business Machines" asserts that this content is safe. You should only install/view this content if you trust "International Business Machines" to make that assertion.

Figure 5-18 Java 2 Plug-in security warning

5.10 Java 2 practical issues

This section addresses practical issues involved in using Java 2 version of Host On-Demand. The information in this section is relatively brief and at a high level. For more specific, detailed information:

- On client Java types (Java 1, Java 2, Autodetect), see 5.11, "Client Java type: Java 1, Java 2, or Autodetect" on page 192, and 5.12, "Effect of client Java type at startup" on page 194.
- On the Java 2 download client, see 5.15, "The Java 2 download client" on page 212.
- On the Java 2 cached client, see 5.14, "The Java 2 cached client" on page 203.
- On removing the Java 1 and Java 2 cached clients, see 5.14.7, "Removing the cached client" on page 209.

- On browsers, see 5.16, “Web browsers: Java 1 and Java 2 enabled” on page 213.
- On the Java 2 plug-in, see 5.17, “The Java 2 plug-in” on page 218.
- On the Java 2 cache, see 5.18.1, “More information on the new Java 2 cache” on page 227.

5.10.1 Limitations and workarounds

This section describes limitations and workarounds in Java 2 support by Host On-Demand.

Download client

The following limitations exist in Host On-Demand download client support. For the reasons behind these limitations see “Reasons for three limitations on the Java 2 download client” on page 230:

1. When a Java 2 download client is configured with a preload list, no additional components can be downloaded later.

   The workaround is to configure the client so that every component that may be needed is included in the preload list.

   > **Note:** Components in the preload list are downloaded as JAR files. Because JAR files contain compressed data, components that are specified in the preload list are downloaded more quickly than loose class files would be downloaded.

2. The default download clients (such as `HOD_en.html`, `HODCached_en.html`, and so on do not contain the following client components:

   – 5250 file transfer
   – Import/export
   – SLP
   – Thai sessions
   – FTP Codepage Converter
   – Bidirectional sessions
   – 5250 Hindi sessions
   – DBCS sessions using user-defined character settings

   IBM removed these less frequently used components from the preload list of the Java 2 default download HTML files to shorten download time. However, with the Java 2 download client, any component not in the preload list cannot be downloaded later.

If you want some or all of these components to be in the preload list, perform one of the following actions:

- Use the Deployment Wizard to create a download client Java 2 HTML file that contains exactly the components that you need.
- Use the default HTML file for the cached client (HODCached_xx.html, where xx is the two-letter language suffix) instead of the default HTML file for the download client.
- Use the debug version of the default download client (HODDebug_en.html, and so on). The debug version contains all the components. However, the debug version of the default download client is larger than the non-debug version.

Mac OS X limitations

The Mac OS X client does not support the Java 2 cached client improvements described in 5.9.3, “Improvements to the cached client for Java 2” on page 181. For more information on Mac OS X support, refer to 5.2, “Mac OS X clients” on page 159.

Limitations of specific Java 2 plug-ins

The Sun Java 2 plug-in has a limitation with Hindi character conversion. If you need Hindi character conversion, use the IBM Java 2 plug-in.

Limitations with customer-supplied applets and Java 2

If a user runs a customer-supplied applet (that is, an applet written by your company or a third party) with a session (such as 3270 Display) launched from a Java 2 Host On-Demand client, and if this applet requires any Java 2 permissions, then you must take one of the following actions to meet the security requirements of Java 2:

- The applet must be archived in a signed Java 2 .JAR file.
- The permissions must previously have been granted on the workstation using the Java 2 Policy Tool that is provided with the Java 2 plug-in.

If you do not meet the security requirements of Java 2, the applet silently fails.

Limitations with restricted users and Java 2

Restricted users do not have the authority to install the Java 2 plug-in. A user with administrative authority must install the Java 2 plug-in.

5.10.2 Effects on system resources

Running the Java 2 version of Host On-Demand affects the client system in the following ways:

- A slightly longer time is required before the Host On-Demand desktop appears.

  The delay is due to facts such as:

  - If the client Java type is Java 2 or Autodetect, then the HTML file has to detect the browser type and determine whether the Java 2 plug-in is present.
  - The Java 2 plug-in has to be loaded.

- Additional disk space is required if the Java 2 cached client attaches to multiple servers.

  The reason is that the Java 2 cached client components are installed in separate directories for each server visited.

  For example, if a user visits two servers running the same level of Host On-Demand, and runs an HTML file that is the same on both servers, then two sets of Host On-Demand components will be stored in the Java 2 cache. Each set will be associated with one of the servers and will be re-used if the user visits the server again.

5.10.3 Must I migrate my existing Deployment Wizard files?

Migration in this section refers to using the Host On-Demand 8.0 Deployment Wizard to regenerate HTML files that were created using previous versions of the the Host On-Demand Deployment Wizard:

- You do not need to migrate HTML files that are used only by clients running Java 1 browsers.

  Specifically we are referring to the following situations:

  - Your clients have been running Java 1 browsers and will continue to do so.
  - You created HTML files using the Host On-Demand 6.0 Deployment Wizard.
  - Your clients have been using these files to connect with a Host On-Demand 6.0 server.
  - Your clients now are going to use these files to connect with a Host On-Demand 8.0 server.

In this situation, you do not need to migrate your files using the Host On-Demand 8.0 Deployment Wizard.

- IBM recommends that you migrate HTML files that are used by clients running Java 2 enabled browsers.

  Specifically, we are referring to the following situation:

  - Your clients have been running Java 2 enabled browsers and will continue to do so.
  - You created HTML files using the Host On-Demand 6.0 Deployment Wizard.
  - Your clients have been using these files to connect with a Host On-Demand 6.0 server.
  - Your clients now are going to use these files to connect with a Host On-Demand 8.0 server.

  In this situation, you actually do not need to migrate your files using Host On-Demand 8.0 Deployment Wizard. Your files will continue to function as they did when your clients attached to a Host On-Demand 6.0 server.

  Unfortunately, this level of functionality means that the Java 2 enabled browsers will download Host On-Demand 8.0 Java 1 code modules, not Java 2 code modules. Your clients will not be able to use any of the Java 2 functionality in Host On-Demand 8.0.

  If you want your clients to use any Java 2 functionality in Host On-Demand 8.0, then you must migrate the HTML files that you created with Host On-Demand 6.0.

  For these reasons, IBM recommends in this situation that you migrate your HTML files.

5.10.4 What if I want to continue running Java 1 browsers only?

If your clients are running Java 1 browsers only, and you want to continue that practice for the time being, then you have only a few tasks, or no tasks to perform:

- Your clients should already be running Netscape 4.x or Internet Explorer without the Java 2 plug-in.
- You do not have to migrate your existing HTML files that you created with the Deployment Wizard from Host On-Demand 6.0. These files will continue to run with Host On-Demand 8.0. See 5.10.3, “Must I migrate my existing Deployment Wizard files?” on page 188.

- If you do want or need to migrate your existing HTML files, use the Deployment Wizard from Host On-Demand 8.0. On the Additional Functions page, set the Client Java Type field to `Java 1`.
- If your clients use one of the default HTML files, such as HOD_en.html or HODCached_en.html, you can improve start up time by making the following change. Edit the HTML files with a text editor as follows:
  - Find the JavaScript line:

    ```
    var hod_JavaType = 'detect' ;
    ```

  - Change it to:

    ```
    var hod_JavaType = 'java1' ;
    ```

  This change will cause the HTML file to immediately launch the Host On-Demand applet on the browser's Java 1 JVM rather than try to detect whether the browser is Java 1 or Java 2 enabled.
- On new workstations:
  - Verify that a Java 1 browser is installed.
  - Verify that the Java 1 browser has access to a Java 1JVM. See 5.16, "Web browsers: Java 1 and Java 2 enabled" on page 213.

5.10.5 What if I am already running Java 2 enabled browsers?

If some or all of your clients are running Java 2 enabled browsers, then you may have a few tasks to perform.

- Your clients should already be running a Java 2 capable browser with a Java 2 plug-in.
- If necessary, for client machines running Internet Explorer, use the Java 2 Plug-in control panel to verify that the default JVM for Internet Explorer is *not* set to the Java 2 plug-in. For more information see "Default JVM for Internet Explorer must be MS Java 1 JVM" on page 216.
- Although your existing Java 2 HTML files run on Host On-Demand 8.0, they will continue to download Java 1 modules just as they did in Host On-Demand 6.0. Therefore, you should migrate your existing HTML files. See 5.10.3, "Must I migrate my existing Deployment Wizard files?" on page 188.
- If you want to or need to migrate your existing HTML files, use the Host On-Demand 8.0 Deployment Wizard. On the Additional Options page:
  - Set the Client Java Type field to Java 2 if *all* your clients are using Java 2 enabled browsers, or

  - Set the Client Java Type field to Autodetect if some of your clients are using Java 2 enabled browsers and others are using Java 1 browsers, or if you are not sure.

- Users should remove any previous Java 1 cached client or Java 2 cached client from their workstations.
- On new workstations:
  - Verify that a Java 2 capable browser is installed.
  - Verify that a Java 2 plug-in is installed.
  - For Internet Explorer, use the Java 2 Plug-in control panel to verify that Internet Explorer's default JVM is *not* set to the Java 2 plug-in. For more information, see “Default JVM for Internet Explorer must be MS Java 1 JVM” on page 216.

5.10.6 What if I want to migrate my users to Java 2 enabled browsers?

If all your clients are running Java 1 browsers, and you want to change some or all of your clients to Java 2 enabled browsers, you have a few tasks to perform:

- You probably want your clients that are changing to Java 2 enabled browsers to download the Java 2 version of Host On-Demand, rather than to download Java 1 modules as in Host On-Demand 6.0. Therefore, you should migrate your existing HTML files. See 5.10.3, “Must I migrate my existing Deployment Wizard files?” on page 188.
- If you want to or need to migrate your existing HTML files, use the Deployment Wizard from Host On-Demand 8.0. On the Additional Options page:
  - Set the Client Java Type field to Java 2 if *all* your clients are using Java 2 enabled browsers, or
  - Set the Client Java Type field to Autodetect if some of your clients are using Java 2 enabled browsers and others are using Java 1 browsers, or if you are not sure.
- Users should remove any previous Java 1 cached client or Java 2 cached client from their workstation.
- On all workstations that will use Java 2:
  - Verify that a Java 2 capable browser is installed.
  - Verify that a Java 2 plug-in is installed.
  - If necessary, for client machines running Internet Explorer, use the Java 2 Plug-in control panel to verify that Internet Explorer’s default JVM is *not*

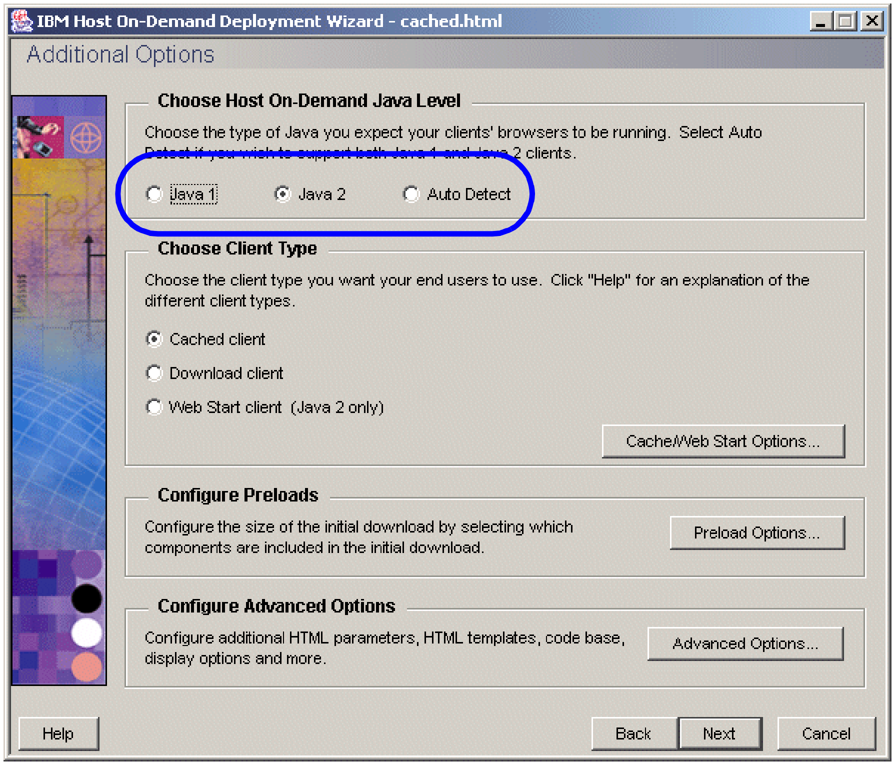
set to the Java 2 plug-in. For more information, see “Default JVM for Internet Explorer must be MS Java 1 JVM” on page 216.

5.11 Client Java type: Java 1, Java 2, or Autodetect

Host On-Demand 7.0 added to the Deployment Wizard the concept of a client Java type. The possible settings for client Java type are: Java 1, Java 2, and Autodetect.

5.11.1 Overview

The Client Java Type field appears on the Additional Options page of the Deployment Wizard. This page is shown in the figure below. The client Java type is set to `Java 1`.



IBM Host On-Demand Deployment Wizard - cached.html

Additional Options

Choose Host On-Demand Java Level

Choose the type of Java you expect your clients' browsers to be running. Select Auto Detect if you wish to support both Java 1 and Java 2 clients.

○ Java 1 ● Java 2 ○ Auto Detect

Choose Client Type

Choose the client type you want your end users to use. Click "Help" for an explanation of the different client types.

● Cached client

○ Download client

○ Web Start client (Java 2 only)

Configure Preloads

Configure the size of the initial download by selecting which components are included in the initial download.

Configure Advanced Options

Configure additional HTML parameters, HTML templates, code base, display options and more.

Figure 5-19 Deployment Wizard page showing Client Java Type field

The following sections discuss the client Java types. For the specific effect that each of these settings has at startup, see 5.12, “Effect of client Java type at startup” on page 194.

5.11.2 Java 1 client type

Choose this setting if you know that all your Host On-Demand clients are running Java 1 browsers.

Choosing this setting instead of Autodetect will save your clients the small (except for slower systems) appreciable time that is required for the HTML file to detect whether the client browser type is Java 1 or Java 2 enabled.

In one unusual situation you must choose the Java 1 setting rather than Autodetect. These situation, which are also described in the online documentation, are:

- Your deployment uses the configuration server-based model.
- Your server has been running Host On-Demand 6.0.x or earlier.
- You are now installing Host On-Demand 8.0 on the server.
- You want to use cached-client controls so that not all Java 1 clients are upgraded on their first try (deferred upgrades).

In this situation, you must specify Java 1 rather than Autodetect. If you specify Autodetect, your clients will not be able to run Host On-Demand properly. Alternatively, you can change your HTML file settings not to use deferred upgrades.

After all your clients have upgraded to Host On-Demand 8.0, you are no longer exposed to this problem. At this point you can change the client Java type of the HTML file from Java 1 to Autodetect if you wish.

5.11.3 Java 2 client type

Choose this setting if you know that all your Host On-Demand clients are running Java 2 enabled browsers.

Choosing this setting instead of Autodetect will save your clients the small (except for slower systems) appreciable time that would be required for the HTML file to detect whether the client browser type is Java 1 or Java 2 enabled.

Choosing this setting will also require your users, or in some scenarios merely remind them to use a Java 2 enabled browser in order to take advantage of the capabilities of the Java 2 version of Host On-Demand.

Note: Occasionally a problem occurs that causes the HTML file to fail to detect the Java 2 plug-in when it is in fact present. As a result the HTML file behaves at startup as if the Java 2 plug-in were not installed. The workaround is to retry the operation. The detection usually succeeds on the second try.

5.11.4 Autodetect client type

Choose this setting if you know that some of your Host On-Demand clients are using Java 1 browsers while other clients are using Java 2 enabled browsers, or if you are not sure.

Choosing this setting instead of Java 1 or Java 2 will allow both types of clients to use Host On-Demand, but will also impose a small but, for slower systems, appreciable delay while the HTML file detects whether the client browser type is Java 1 or Java 2 enabled.

For an unusual situation in which you must use Java 1 instead of Autodetect, see section 5.11.2, “Java 1 client type” on page 193.

Attention: Autodetect checks for a installed Java 2 environment. If it finds a Java 2 environment, the Java 2 client will be used, regardless of whether the Java 2 environments is enabled or not.

5.12 Effect of client Java type at startup

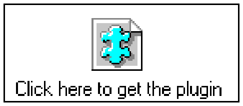
The tables in this section show what occurs at startup for each client Java type. The results depend not only on the client Java type, but also on the browser type and whether the client is a download client or a cached client.

These tables assume that Internet Explorer’s default JVM is set to the Microsoft Java 1 JVM. For more information on this topic, see “Default JVM for Internet Explorer must be MS Java 1 JVM” on page 216.

5.12.1 Messages

The figure below shows the message displayed when:

- The client Java type is Java 1 or Java 2.
- The browser is Netscape 6.x without a Java 2 plug-in.
- The client is a download client or a cached client.



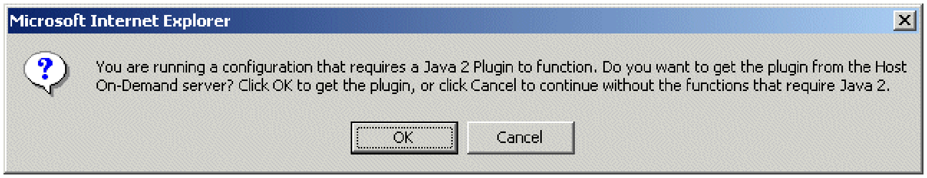
Click here to get the plugin

Figure 5-20 Netscape 6.x message prompting user to download a Java 2 plugin

The next figure shows the messages displayed when:

- The client Java type is Java 2.
- The browser is Netscape 4.x or Internet Explorer without the Java 2 plugin.
- The client is a download client or a cached client.
- The platform is Win32.

The following figure shows the message for the Win32 platform.



Microsoft Internet Explorer

You are running a configuration that requires a Java 2 Plugin to function. Do you want to get the plugin from the Host On-Demand server? Click OK to get the plugin, or click Cancel to continue without the functions that require Java 2.

Figure 5-21 You are running a configuration that requires a Java 2 Plug-in to function

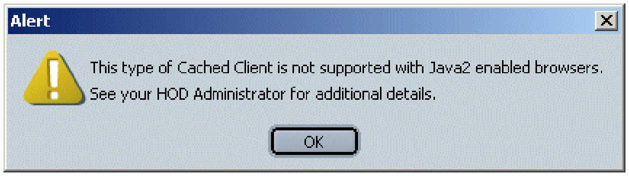
A similar message is shown in the same situation for the non-Win32 platform, but the user is told to contact the system administrator in order to get the plug-in.

Example 5-2 Non-Win32 platform message

```
You are running a configuration that requires a Java 2 Plugin to function.
Please contact your administrator to obtain the necessary Java 2 Support.  Host
On-Demand will continue without the functions that require Java 2.
```

The figure below shows the message displayed when:

- The client Java type is Java 1.
- The browser is Netscape 6.x with a Java 2 plug-in.
- The client is a cached client.



Alert

This type of Cached Client is not supported with Java2 enabled browsers.
See your HOD Administrator for additional details.

Figure 5-22 This type of cached client is not supported with Java 2 enabled browsers

5.12.2 Startup behavior for Java 1 download client

The table below shows the startup behavior for the Java 1 download client based on the client Java type and the browser type.

Table 5-5 Startup behavior for Java 1 download client

Client Java type in Deployment Wizard:	**Browser type:**	**Result:**
Java 1 or Autodetect	Netscape 4.x	HTML file runs Java 1 download client
Java 1 or Autodetect	Internet Explorer without Java 2 plug-in	HTML file runs Java 1 download client
Java 1	Internet Explorer with Java 2 plug-in	HTML file runs Java 1 download client
Java 1 or Autodetect	Netscape 6.x without Java 2 plug-in	Netscape 6.x displays warning message in Figure 5-20 on page 195. User options: - Quit; or - Click to download Sun Java 2 plug-in
Java 1	Netscape 6.x with Java 2 plug-in	HTML file runs Java 1 download client

5.12.3 Startup behavior for Java 2 download client

The table below shows the startup behavior for the Java 2 download client based on the client Java type and the browser type.

Table 5-6 Startup behavior for Java 2 download client

Client Java type in Deployment Wizard:	**Browser type:**	**Result:**
Java 2	Netscape 4.x	HTML file displays warning message, see Figure 5-21 on page 195. User options if Win32 platform: - Cancel; or - Run Java 1 download client; or - Download IBM Java 2 plug-in for Win32 User options if non-Win32 platform - Cancel; or - Run Java 1 download client

Client Java type in Deployment Wizard:	**Browser type:**	**Result:**
Java 2	Internet Explorer without Java 2 plug-in	HTML file displays warning message, see Figure 5-21 on page 195. User options if Win32 platform: - Cancel; or - Run Java 1 download client; or - Download IBM Java 2 plug-in for Win32 User options if non-Win32 platform - Cancel; or - Run Java 1 download client
Java 2 or Autodetect	Internet Explorer with Java 2 plug-in	HTML file runs Java 2 download client
Java 2 or Autodetect	Netscape 6.x without Java 2 plug-in	Netscape 6.x displays warning message, see Figure 5-20 on page 195. User options: - Quit; or - Download Sun Java 2 plug-in
Java 2 or Autodetect	Netscape 6.x with Java 2 plug-in	HTML file runs Java 2download client

5.12.4 Startup behavior for Java 1 cached client

The table below shows the startup behavior for the Java 1 cached client based on the client Java type and the browser type.

Table 5-7 Startup behavior for Java 1 cached client

Client Java type in Deployment Wizard:	**Browser type:**	**Result:**
Java 1 or Autodetect	Netscape 4.x	HTML file installs Java 1 cached client. User restarts browser. HTML file launches Java 1 cached client.
Java 1 or Autodetect	Internet Explorer without Java 2 plug-in	HTML file installs Java 1 cached client. User restarts browser. HTML file launches Java 1 cached client.
Java 1	Internet Explorer with Java 2 plug-in	HTML file installs Java 1 cached client. User restarts browser. HTML file launches Java 1 cached client.

Client Java type in Deployment Wizard:	Browser type:	Result:
Java 1 or Autodetect	Netscape 6.x without Java 2 plug-in	Netscape 6.x displays warning message, see Figure 5-20 on page 195. User options: - Quit; or - Click to download Sun Java 2 plug-in
Java 1	Netscape 6.x with Java 2 plug-in	HTML file: - Displays error message, see Figure 5-22 on page 195. - Refuses to install cached client. User option: - Quit, then see system administrator.

5.12.5 Startup behavior for Java 2 cached client

The table below shows the startup behavior for the Java 2 cached client based on the client Java type and the browser type.

Table 5-8 Startup behavior for Java 2 cached client

Client Java type in Deployment Wizard:	Browser type:	Result:
Java 2	Netscape 4.x	1) HTML file displays warning message, see Figure 5-21 on page 195. User options if Win32 platform: - Cancel; or - Choose to install Java 1 cached client; or - Download IBM Java 2 plug-in for Win32 User options if non-Win32 platform - Cancel; or - Choose to install Java 1 cached client 2) Assume: user chooses to install Java 1 cached client. 3) HTML file installs and launches Java 1 cached client.

Client Java type in Deployment Wizard:	Browser type:	Result:
Java 2	Internet Explorer without Java 2 plug-in	1) HTML file displays warning message, see Figure 5-21 on page 195. User options if Win32 platform: - Cancel; or - Choose to install Java 1 cached client; or - Download IBM Java 2 plug-in for Win32 User options if non-Win32 platform - Cancel; or - Choose to install Java 1 cached client 2) Assume: user chooses to install Java 1 cached client. 3) HTML file installs and launches Java 1 cached client.
Java 2 or Autodetect	Internet Explorer with Java 2 plug-in	HTML file installs and launches Java 2 cached client.
Java 2 or Autodetect	Netscape 6.x without Java 2 plug-in	Netscape 6.x displays warning message, see Figure 5-20 on page 195. User options: - Quit; or - Click to download Sun Java 2 plug-in
Java 2 or Autodetect	Netscape 6.x with Java 2 plug-in	HTML file installs and launches Java 2 cached client.

5.13 Download client and cached-client implementation

This section describes:

- The applets that are launched for the download client and the cached client.
- How the Host On-Demand components are stored for the download client and the cached client.

For more details, see 5.18.4, “More information on launching the Host On-Demand applets” on page 232.

5.13.1 HostOnDemand applet and CachedAppletSupport applet

The HostOnDemand applet

The HostOnDemand applet is the applet that is launched for a download client by the HTML file. The actual class file for the Java 1 version of Host On-Demand is `HostOnDemand.class`, and the actual class file for the Java 2 version of Host On-Demand is a separate module that is also named `HostOnDemand.class`. When the HostOnDemand applet is launched, the applet puts up the appropriate version (Java 1 or Java 2) of the Host On-Demand desktop, and manages the desktop and sessions.

When the download client is running, if the JVM is Java 1, and there is a preload list and an additional component is needed, the browser downloads from the server the loose class files that make up the component. In contrast, if the JVM is Java 2, no additional components can be downloaded. See 5.15, “The Java 2 download client” on page 212.

The CachedAppletSupport applet

The CachedAppletSupport applet is the applet that is launched for a cached client by the HTML file. The actual class file for the Java 1 version of Host On-Demand is `CachedAppletSupportApplet.class`, and the actual class file for the Java 2 version of Host On-Demand is `CachedAppletLoader.class`.

When the CachedAppletSupport applet is launched, it checks whether the cached client components have been installed. If not, then the CachedAppletSupport applet installs the cached client components. Then it either tells the user to restart the browser in order to start the cached client (if this is the Java 1 CachedAppletSupport applet) or else it immediately starts the cached client (if this is the Java 2 CachedAppletSupport applet). To start the cached client, the CachedAppletSupport applet launches the HostOnDemand applet, the same applet that is used for the download client.

When the cached client is running, whether the JVM is Java 1 or Java 2, if there is a preload list, and an additional component is needed, the CachedAppletSupport applet arranges for the component to be downloaded from the server. Then the user must restart the browser.

5.13.2 How Host On-Demand component modules are stored

A component is a functional unit, such as 3270 Display Sessions or 3270 Printer Sessions. A component is made up of one or possibly more than one downloadable module.

A downloadable module may be:

- A signed archive file, such as a JAR file or a CAB file, which contains a collection of related individual Java class files; or
- An individual Java class file. The class file may be a Java 1 class file (that is, created by a Java 1 compiler) or a Java 2 class file (that is, created by a Java 2 compiler).

The following table summarizes how the modules that make up Host On-Demand components are downloaded and stored for the Java 1 and Java 2 download clients and cached clients.

Table 5-9 How components are downloaded and stored

JVM:	Download client:	Cached client:
Java 1	Components in the preload list are downloaded as JAR or CAB files containing Java 1 class files.	Components in the preload list are downloaded as JAR or CAB files containing Java 1 class files.
	Components not in the preload list are downloaded as Java 1 class files.	Components not in the preload list are likewise downloaded as JAR or CAB files containing Java 1 class files
	Downloaded JAR or CAB files are not unpacked.	For Internet Explorer, Host On-Demand unpacks the class files from each CAB file. For Netscape 4.x, the class files are not unpacked from the JAR files.
	The modules reside in the browser cache.	The modules reside in a user directory.
	Each component, whether in the preload list or downloaded as needed, is downloaded anew each time the download client is run.	Each component, whether in the preload list or downloaded as needed, is downloaded once.

JVM:	Download client:	Cached client:
Java 2	-- Components in the preload list are downloaded as JAR files containing Java 2 class files.	-- Components in the preload list are downloaded as JAR files containing Java 2 class files.
	-- Components not in the preload list cannot be downloaded later.	-- Components not in the preload list are likewise downloaded as JAR files containing Java 2 class files.
	-- The class files are not unpacked from the JAR files.	-- The class files are not unpacked from the JAR files.
	-- Components reside in the Java 2 plug-in's temporary cache.	-- Components reside in the HOD's own Java 2 cache.
	-- Each component is downloaded anew each time the download client is run.	-- Each component, whether in the preload list or downloaded as needed, is downloaded once.

Download client

For the Java 1 download client, components in the preload list are downloaded as JAR (for Netscape) or CAB (for Internet Explorer) files containing Java 1 class files. The class files remain in the JAR or CAB files. In contrast, components not in the preload list are downloaded as individual Java 1 class files. All the downloaded modules, including JAR or CAB files and loose class files, reside in the browser cache. An example of a JAR and a CAB file are habasen.jar and habasen.cab.

For the Java 2 download client, components in the preload list are downloaded as JAR files containing Java 2 class files. The class files are not unpacked, but rather remain in the JAR files. Components not in the preload list cannot be downloaded later. The JAR files reside in the Java 2 plug-in's temporary cache. These Java 2 JAR files have names that are similar to the names of the Java 1 JAR files, but are distinguished by a 2 appended to the file name. An example is habasen2.jar.

For both Java 1 and Java 2 enabled browsers, each component, whether in the preload list or downloaded as needed, is downloaded anew each time the download client is run.

When the Java 1 or Java 2 download client is running, and the JVM needs to find a Host On-Demand class file, the JVM first looks among the loose class files if there are any. If the class file is not found, the JVM then looks among the Host On-Demand JAR files until it finds the correct one, and then finds the class file within the JAR file.

The Java 1 and Java 2 download clients do not interfere with each other because the Java 1 downloaded modules and the Java 2 downloaded modules have different names, and are stored in different places.

Cached client

The Java 1 and Java 2 cached clients use the same modules as their download client counterparts, but store the modules differently.

For the Java 1 cached client, components in the preload list are downloaded as JAR or CAB files containing Java 1 class files. Components not in the preload list are likewise downloaded as JAR or CAB files containing Java 1 class files. For Internet Explorer, Host On-Demand unpacks the class files from each CAB file. For Netscape 4.x, the class files are not unpacked from the JAR files. The files, whether loose class files or JAR files, reside in a user directory. But the user directory is different for Internet Explorer than for Netscape 4.x.

For the Java 2 cached client, components in the preload list are downloaded as JAR files containing Java 2 class files. Components not in the preload list are likewise downloaded as JAR files containing Java 2 class files. The class files are not unpacked but remain in the JAR files. The JAR files reside in HOD’s new Java 2 cache. See 5.18.1, “More information on the new Java 2 cache” on page 227 for more information.

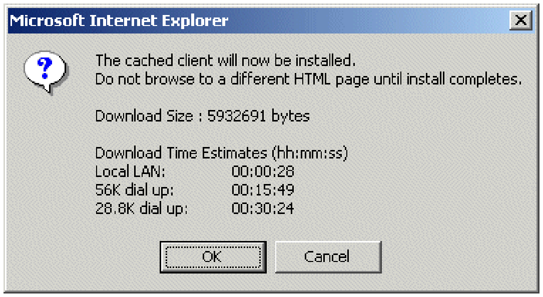
For both Java 1 and Java 2 enabled browsers, each component, whether in the preload list or downloaded as needed, are downloaded once.

The Java 1 and Java 2 cached clients do not interfere with each other because the Java 1 downloaded modules and the Java 2 downloaded modules have different names and are stored in different places.

For more information on how the modules are stored for the Java 1 and Java 2 cached clients, see 5.14.5, “Handling cached client components for Java 1 and Java 2” on page 207.

5.14 The Java 2 cached client

When the Java 2 cached client is started the first time it displays a message similar to the one shown in the figure below. The text is the same whether the cached client is for Java 1 or Java 2, but the download sizes are different for Java 1 and Java 2. The figure below shows the message displayed by Internet Explorer for the Java 2 cached client:


Microsoft Internet Explorer

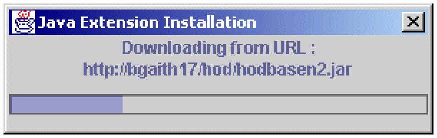
The cached client will now be installed.
Do not browse to a different HTML page until install completes.

Download Size : 5932691 bytes

```
Download Time Estimates (hh:mm:ss)
Local LAN:        00:00:28
56K dial up:      00:15:49
28.8K dial up:    00:30:24
```

Figure 5-23 Install cached client

However, when the user clicks **OK** and the installation begins, the Java 2 cached client does *not* display the progress indicator frame displayed by the Java 1 cached client. Instead, the words `Loading Java Applet ...` appear in the middle of the Host On-Demand desktop. Also, some type of indicator may appear as each component is downloaded. For example, the following indicator is displayed when a component is downloaded by Internet Explorer running with the IBM Java 2 plug-in as shown in Figure 5-24.


Java Extension Installation

Downloading from URL :
http://bgaith17/hod/hodbasen2.jar

Figure 5-24 Indicator displayed by Internet Explorer running with Java 2 plug-in

When the installation is complete, the Host On-Demand applet is launched immediately. The user does not have to restart the browser.

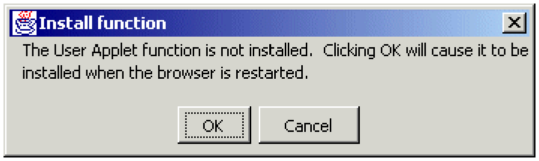
5.14.1 Java 2 cache options

Like the Java 1 cached client, the Java 2 cached client supports the following cache options:

- Control of user upgrades
- Debug cached client installation process
- Upgrade in the background (except when migrating from HOD 7 to HOD 8)

5.14.2 Downloading a Java 2 component not on the preload list

If the user attempts to use a Java 2 component not on the preload list, a message is displayed. For example, the figure below shows the message displayed when the Run Applet component is not on the preload list and the user starts a session and clicks **File, Run Applet**. This is the message displayed with Java 2, but the same message is displayed with Java 1.



The User Applet function is not installed. Clicking OK will cause it to be installed when the browser is restarted.

Figure 5-25 Message displayed a for component that is not on the preload list

When the user clicks **OK**, Host On-Demand modifies the caching list so that the component will be downloaded when the browser is restarted. The user must restart the browser.

The following table compares this operation on the Java 1 version of Host On-Demand and on the Java 2 version.

Table 5-10 Downloading a component not on the preload list

Item:	**Java 1 cached client:**	**Java 2 cached client:**
OK/Cancel message is displayed:	Yes	Yes
Update method:	Component is downloaded immediately.	Caching list is updated. Component is downloaded when browser is restarted.
User must restart browser:	Yes	Yes

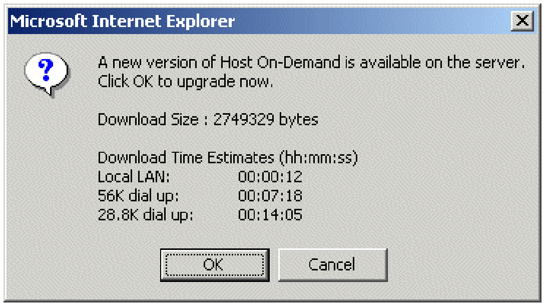
5.14.3 Java 2 cached client does not interfere with download client

The Java 2 cached client does not interfere with the Java 2 download client. That is, the user can run the Java 2 download client without first removing the Java 2 cached client.

The reason is that the Java 2 download client's components are stored in the Java 2 plug-in's temporary cache, while the Java 2 cached client's components are stored on disk using separate directories for each server. For more information about how component modules are stored, see 5.13.2, "How Host On-Demand component modules are stored" on page 200.

5.14.4 Java 2 cached client upgrades

When the Java 2 cached client detects a newer version of Host On-Demand on the server, a message such as the one in Figure 5-26. This is the message displayed when the cached client is running on Internet Explorer.


Microsoft Internet Explorer

A new version of Host On-Demand is available on the server.
Click OK to upgrade now.

Download Size : 2749329 bytes

```
Download Time Estimates (hh:mm:ss)
Local LAN:          00:00:12
56K dial up:        00:07:18
28.8K dial up:      00:14:05
```

Figure 5-26 Upgrade message

The upgrade takes place in the foreground. When the upgrade is complete, the Host On-Demand desktop is displayed. The browser does not have to be restarted.

Avoiding an extra download going from Java 1 to Java 2

If you are migrating users from Java 1 browsers to Java 2 browsers, and you are also upgrading the level of Host On-Demand on the server from Host On-Demand 6.x to Host On-Demand 8.0, then you can prevent your users from having to download their cached clients twice by migrating users to Java 2 browsers before they connect to the Host On-Demand 8.0 server.

Compare the following two procedures.

1. This procedure requires users to download a new cached client twice:
   - The user is running a Java 1 browser.
   - The user already has a Java 1 cached client installed from Host On-Demand 6.0.
   - The user connects to a server HODSRV1 running Host On-Demand 8.0. At this point, the Host On-Demand 8.0 Java 1 cached client has to be downloaded.

- Now the system administrator installs a Java 2 enabled browser and a Java 2 plug-in on the user's machine.
- The user again connects to HODSRV1. At this point the Host On-Demand 8.0 Java 2 cached client has to be downloaded. This is the second download.

2. In contrast, the following procedure requires users to download a new cached client only once:
   - The user is running a Java 1 browser.
   - The user already has a Java 1 cached client installed from Host On-Demand 6.0.
   - Now the system administrator installs a Java 2 enabled browser on the user's machine.
   - The user connects to a server HODSRV1 running a newer version of Host On-Demand. At this point the Host On-Demand 8.0 Java 2 cached client has to be downloaded. This is the first and only download.

5.14.5 Handling cached client components for Java 1 and Java 2

The table below summarizes how the Host On-Demand components are handled by the Java 1 and Java 2 cached clients.

Table 5-11 How components are handled by the Java 1 and Java 2 cached clients

Item:	Java 1 cached client	Java 2 cached client
Modules are downloaded as:	JAR or CAB files containing class files compiled by the Java 1 compiler.	JAR files containing class files compiled by the Java 2 compiler.
Where the Java class files are kept:	Unpacked as loose class files in a browser-specific user work area (Internet Explorer) or packed in JAR files in a browser-specific user work area (Netscape 4.x).	Packed in JAR files in HOD's cache.
Cache management file name:	HOD_CCR.ccr	server.dirname.HOD_CCR2.ccr
Are components associated with a server?	No	Yes

Java 1 cached client

For the Java 1 cached client each component is downloaded as one or more signed archives (a JAR file for Netscape, a CAB file for Internet Explorer).

For Internet Explorer, the class files are unpacked from the CAB files and stored in a user work area under a subdirectory called HODCC. On Windows 2000 the HODCC subdirectory is located in a path such as the following where JASmith is the user name:

```
c:\Documents and Settings\JASmith\HODCC
```

The individual class files are placed in appropriate subdirectories under the HODCC subdirectory depending on the complete name of the Java package to which the class files belong.

For Netscape 4.x, the class files are not unpacked but remain in the JAR files. The JAR files are stored under a directory in a user work area. On Windows 2000 the directory is located in a path such as the following where JASmith is the user name:

```
c:\Program Files\Netscape\Users\JASmith\cache
```

The component name, file version, and other information about each downloaded JAR or CAB file are stored in a file named HOD_CCR.ccr, which resides in a subdirectory close to the data. On Windows 2000 the HOD_CCR.ccr file for Internet Explorer is located in a path such as the following where JASmith is the user name:

```
c:\Documents and Settings\JASmith\HOD_CCR.ccr
```

On Windows 2000 the `HOD_CCR.ccr` file for Netscape 4.x is located in a path such as the following:

```
c:\Program Files\Netscape\Users\HOD_CCR.ccr
```

Java 2 cached client

For the Java 2 cached client, each component is downloaded as one or more Java 2 JAR files (whether the browser is Netscape 6.x or Internet Explorer with the Java 2 plug-in). The JAR files are placed in HOD's own Java 2 cache using separate directories for each server that the user visits. For more information on the cache, see 5.18.1, "More information on the new Java 2 cache" on page 227. For both Netscape 6.x and Internet Explorer with the Java 2 plug-in, the JAR file is not unpacked into loose class files, and therefore a HODCC directory is not created.

The module name, file version number, and other information about each downloaded JAR file are stored in a file named `server.dirname.HOD_CCR2.ccr`, where `server` is the Host On-Demand server's name and `dirname` is the name of the server's public directory. For example, the file might be named `HODSRV1.hod.HOD_CCR2.ccr`, where `HODSRV1` is the server's TCP/IP hostname and `hod` is the server's public directory. This file is located in the same directory as where the Java 1 `HOD_CCR.ccr` file is located for the Java 1 cached client for Internet Explorer. On Windows 2000 the `HOD_CCR2.ccr` file is located on a path such as the following where JASmith is the user name:

```
c:\Documents and Settings\JASmith\HODSRV1.hod.HOD_CCR2.ccr
```

The same path is used for both Netscape 6.x and Internet Explorer with the Java 2 plug-in.

For Java 2 there will be a separate `server.dirname.HOD_CCR2.ccr` file for each Host On-Demand server visited by the user, just as there are separately downloaded JAR files in the cache directory for each Host On-Demand server visited.

5.14.6 Increased flexibility with Java 2 cached clients

Because Host On-Demand stores the JAR files and separate `HOD_CCR2.ccr` files in separate directories for each Host On-Demand server visited, the Java 2 cached client is not exposed to the same problems that the Java 1 cached client is exposed to when the user visits several Host On-Demand servers running different service levels of Host On-Demand. See "Java 1 cached client support across the Internet" on page 157.

Users who are running the Java 2 cached client can switch among several different servers running different service levels of Host On-Demand without having to remove and re-install the cached client.

Also, the user can switch back and forth between download and cached clients without having to remove the cached client code.

5.14.7 Removing the cached client

Why does the Java 1 cached client need to be removed?

In the following sections are situations justifying removal or non-removal of the cached client.

Situations requiring removal

There are at least two situations in which the Java 1 cached client needs to be removed:

- If the client is running a Java 1 browser, and the cached client is installed, then the download client cannot be run until the cached client is removed.

  For the reason for this limitation, see “Reason for restriction on Java 1 download client” on page 230.

- Certain upgrade scenarios require the cached client to be removed.

  For one such scenario, see “Scenario requiring Java 1 cached client to be removed” on page 229.

Situations not requiring removal

The Java 1 cached client does not need to be removed in order for the Java 2 cached client to be installed. As described in 5.14.5, “Handling cached client components for Java 1 and Java 2” on page 207, the components and caching information for the Java 1 cached client are maintained in different files than the components and caching information for the Java 2 cached client.

However, if a user migrates to a Java 2 enabled browser and does not plan to use the Java 1 cached client data again, then the user might want to remove the Java 1 cached client in order to free up a few megabytes of disk space.

Why does the Java 2 cached client need to be removed?

As mentioned earlier, the Java 2 cached client does not need to be removed in order for the Java 2 download client to be run. See 5.14.3, “Java 2 cached client does not interfere with download client” on page 205.

Nor does the Java 2 cached client need to be removed in order for an earlier version of the cached client modules to be downloaded from a different server. The reason that this problem does not exist for the Java 2 cached client is that the Java 2 plug-in downloads a separate set of components for each server visited. See 5.14.5, “Handling cached client components for Java 1 and Java 2” on page 207.

A scenario in which the user would want to remove the cached client is for a disk cleanup.

Which removal option?

The HTML file `HODMain.html` displays two choices for removing the cached client (see Figure 5-1 on page 150):

- Remove Cached Client (if Java 2 is detected, it removes Java 2, else removes Java 1)
- Remove Cached Client (Java 1 only)

The first option works similar to “Autodetect Java 2” and may confuse some users. In fact, the removal process is checking for a Java 2 environment to be installed. If yes, regardless of whether it is being used for HOD, it tries to remove the Java 2 cached client. So the user might need to know that he has a Java 2 environment installed, but is using Java 1 for HOD, and therefore has to use the second option.

In contrast, the second option will remove the Java 1 cached client data.

The following table summarizes the effect of these options for each browser.

Table 5-12 Effect of selecting a remove option

Browser:	**Remove cached client (if Java 2 is detected, removes Java 2, else removes Java 1)**	**Remove cached client (Java 1 only)**
Netscape 4.x	Removes Java 1 cached client data.	Removes Java 1 cached client data.
Internet Explorer without the Java 2 plug-in	Removes Java 1 cached client data.	Removes Java 1 cached client data.
Netscape 6.x	Removes Java 2 cached client data.	No effect
Internet Explorer with the Java 2 plug-in	Removes Java 2 cached client data.	Removes Java 1 cached client data.

Scenario that may cause confusion

This subsection discusses a potentially confusing scenario that occurs when the user is running Internet Explorer and has the Java 2 plug-in installed, but uses an HTML file that has a client Java type of Java 1 and which launches a cached client:

- Because the client Java type is Java 1, the HTML file will launch Internet Explorer’s default JVM, which is normally the Microsoft Java 1 JVM. See 5.16.3, “Microsoft Web browsers: Internet Explorer” on page 215.
- Therefore, the Java 1 cached client will be installed, not the Java 2 cached client. The user may or may not realize this.

- Now suppose that the user wants to remove the cached client and chooses the first remove option, that is, if Java 2 is detected, it removes Java 2, else removes Java 1.
- Because the Java 2 plug-in is installed, the remove option detects the browser as a Java 2 enabled browser.
- Therefore, the remove option tries to remove Java 2 cached client data, rather than the Java 1 cached client data that is actually installed.
- The Java 1 cached client data is not removed.

To avoid this problem, the user should be warned about this scenario if the HTML file's client Java type is Java 1, and the user is running Internet Explorer with the Java 2 plug-in installed.

Removing the cached client

If the Java 2 plug-in is installed and the user chooses the first remove option, Host On-Demand will remove the `HOD_CCR2.ccr` file and do other cleanup, but the user must manually remove the Java 2 JAR files in the disk directory used for this server.

Removing a cached client shared by multiple users

If multiple users share a single cached client, and one of these users removes the cached client, then the cached client is removed for all users. For information on sharing a single cached client, refer to "Sharing the cached client on the Windows platform" on page 154.

5.15 The Java 2 download client

Most of the material for the Java 2 download client has already been covered. Recall that:

- The Java 2 download client can be run without removing the Java 2 cached client. See 5.9.3, "Improvements to the cached client for Java 2" on page 181.
- The startup behavior of the Java 1and Java 2 download clients is governed by the client Java type. See 5.12.2, "Startup behavior for Java 1 download client" on page 196, and 5.12.3, "Startup behavior for Java 2 download client" on page 196.
- The components for Java 2 download clients are downloaded as Java 2 JAR files, and are stored in the Java plug-in's temporary cache. See 5.13.2, "How Host On-Demand component modules are stored" on page 200.
- The following limitations exist in Host On-Demand support for the Java 2 download client (see 5.10.1, "Limitations and workarounds" on page 186). For

a discussion of the reasons for these limitations, see “Reasons for three limitations on the Java 2 download client” on page 230:

- No component can be downloaded that is not on the preload list.
- The default download clients (HOD_en.html, and so on) do not include some components.

5.16 Web browsers: Java 1 and Java 2 enabled

When a Host On-Demand HTML file with a client type of Java 2 or Autodetect is run, it launches a detection applet in order to detect whether a Java 2 plug-in is installed. A JVM must be present in order for this detection applet to be run.

Therefore, you must ensure that a Java JVM as well as a supported Web browser is installed on your Host On-Demand client machines.

Java 1 browsers, such as Netscape 4.x and Internet Explorer without the Java 2 plug-in, usually have a Java 1 JVM module included with them. Netscape 4.x includes a Symantec Java 1 JVM. Internet Explorer includes a Microsoft Java 1 JVM. However, be aware that in an early version of Windows XP the Java 1 JVM was not included with Internet Explorer. You had to download and install the JVM separately.

Java 2 enabled browsers, such as Netscape 6.x, need the Java 2 plug-in in order to launch a Java 2 applet. With Netscape 6.x you can install the Sun plug-in as part of the Netscape install, or you can install the IBM, Sun, or other vendor’s Java 2 plug-in separately.

Internet Explorer can function as a Java 2 enabled browser or as a Java 1 browser when the Java 2 plug-in is installed. Either the IBM or the Sun Java 2 plug-in can be used.

Note: IBM recommends the IBM Java 2 plug-in for use with Host On-Demand.

Make sure that your client machines have a supported browser with a compatible JVM installed before rolling the machines out to your users.

For more on the Java 2 plug-in, see 5.17, “The Java 2 plug-in” on page 218.

5.16.1 Web browsers supported

The following is a list of browsers that are supported. This list is taken from the document *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301. Check the latest documentation or the Host On-Demand Web site for the most current list:

- Netscape Navigator 4.7, 6.1, 6.2, 7.0
- Microsoft Internet Explorer 4.01 with SP1®, 5.0, 5.1, 5.5, or 6.0
- Netscape Navigator 4.61 for OS/2
- IBM Web Browser for OS/2 V1.2 (supports Java 2)
- Safari
- Mozilla 1.0.2, 1.2.1

5.16.2 Netscape Web browsers

Here is the information on the browsers.

Netscape 4.x and Netscape 6.x

The table below summarizes the information in this subsection.

Table 5-13 Host On-Demand's use of Netscape browsers

Browser:	JVM:	Type of applets that can be run:	Type of applets run by Host On-Demand:	HTML command to launch applet:
Netscape 4.x	Sun Java 1	Java 1	Java 1	`APPLET`
Netscape 6.x	Java 2 plug-in	Java 1 or Java 2	Java 1 or Java 2	`APPLET`

Netscape 4.x, which runs on several platforms, is a Java 1 browser. It executes HTML statements and uses an integrated Symantec Java 1 JVM to run applets. The Java 1 JVM can run Java 1 applets only. The HTML command **APPLET** is used to launch an applet.

Netscape 6.x, which likewise runs on several platforms, is a Java 2 enabled browser. It can execute HTML statements, but needs a separately installed Java 2 plug-in to run applets.

The Java 2 plug-in can run Java 1 applets as well as Java 2 applets. The HTML command **APPLET** is used to launch an applet on Netscape 6.x, whether the applet is a Java 1 applet or a Java 2 applet.

With Netscape 6.x and the required Java 2 plug-in, the Host On-Demand HTML file usually launches the Java 2 version of the Host On-Demand applets (the HostOnDemand applet for the download client, or the CachedAppletSupport applet for the cached client). But in one situation the HTML file launches the Java 1 version of the Host On-Demand applets on the Java 2 plug-in. See 5.12.2, "Startup behavior for Java 1 download client" on page 196.

For more information on how the Host On-Demand applets are launched, see 5.18.4, "More information on launching the Host On-Demand applets" on page 232.

Installing Netscape 6.x

For information on installing Netscape 6.x on the Win32 platform, see "Installing Netscape 6.x on the Win32 platform" on page 225.

5.16.3 Microsoft Web browsers: Internet Explorer

Internet Explorer supports Java 1 and the Java 2 plug-in

The table below summarizes the information in this subsection.

Table 5-14 Host On-Demand's use of Internet Explorer

Browser:	JVM:	Type of applets that can be run:	Type of applets run by Host On-Demand:	HTML command to launch applet:	HTML command used by Host On-Demand:
Internet Explorer without the Java 2 plug-in	Microsoft Java 1	Java 1	Java 1	`APPLET`	`APPLET`
Internet Explorer with the Java 2 plug-in	Java 2 (Sun or IBM)	Java 1 or Java 2	Java 2	`OBJECT` (all Java 2 plug-ins) `APPLET` (newer Sun Java 2 plug-ins)	`OBJECT`

Unlike Netscape, which comes in either a Java 1 (Netscape 4.x) or a Java 2 enabled (Netscape 6.x) version, Internet Explorer is a Java 1 browser that can also use a Java 2 plug-in if one is installed on the system.

Internet Explorer has a setting called the default JVM, which is normally set to be the Microsoft Java 1 JVM. This is the JVM that is included with Internet Explorer. However, the default JVM can be set to be any installed JVM.

Note: Host On-Demand always assumes that Internet Explorer's default JVM is set to the Microsoft Java 1 JVM.

The HTML command **`APPLET`** launches an applet on Internet Explorer's default JVM. The HTML command **`OBJECT`** launches an applet on the Java 2 plug-in. Also, with newer Sun Java 2 plug-ins, the **`APPLET`** command will launch an applet on the Java 2 plug-in.

The Host On-Demand HTML files always use the **`APPLET`** command to launch the Java 1 version of the Host On-Demand applets (the HostOnDemand applet and the CachedClientSupporter applet) and the **`OBJECT`** command to launch the Java 2 versions of the Host On-Demand applets. Note that Host On-Demand could use the **`OBJECT`** command to launch a Java 1 applet on the Java 2 Plug-in's Java 2 JVM, but it does not.

Note: Netscape 6.x also has a default JVM setting. The default JVM is normally set to the Java 2 plug-in when the Java 2 plug-in is installed.

For more information on how the Host On-Demand applets are launched, see 5.18.4, "More information on launching the Host On-Demand applets" on page 232.

Default JVM for Internet Explorer must be MS Java 1 JVM

Some Java 2 plug-ins offer a checkbox that allows the user to switch the browser's default JVM to the Java 2 plug-in.

For Netscape 6.x, you should select this checkbox. However, IBM recommends that you do *not* set this checkbox for Internet Explorer.

Note: IBM recommends that for Internet Explorer running with the Java 2 plug-in, you do *not* set Internet Explorer's default JVM to the Java 2 plug-in.

The reason why, as described in the previous section, is that the Host On-Demand HTML files always assume that the Internet Explorer's default JVM is set to Microsoft's Java 1 JVM. If you set the default JVM to the Java 2 plug-in, Host On-Demand may not run properly. However, there may be situations in which Host On-Demand will run properly with the default JVM set to the Java 2 plug-in.

IBM recommends that you change the settings after the install using the Java Plug-in control panel.

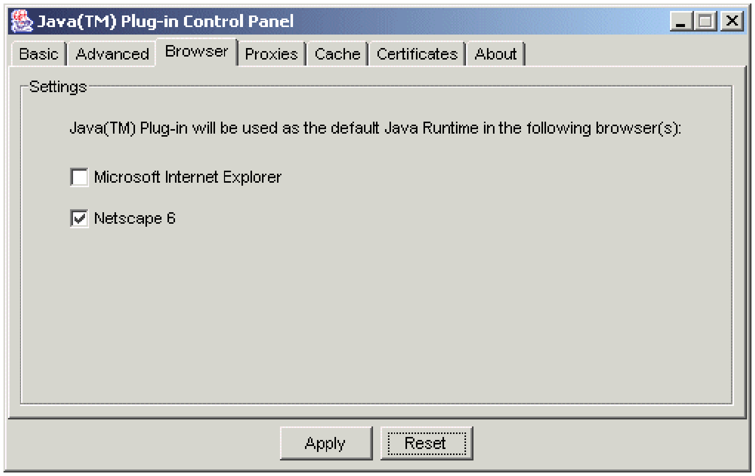
The figure below shows the Browser tab in the Java Plug-in control panel of the IBM 1.4.0 Java 2 plug-in for the Win32 platform. IBM recommends that you set the checkboxes as shown in the figure below. That is:

- Do not check the checkbox for Internet Explorer.

  The default JVM for Internet Explorer will be the Microsoft Java 1 JVM shipped with Internet Explorer.

- Do check the checkbox for Netscape 6.x.

  The default JVM for Netscape 6.x will be the Java 2 plug-in.



Settings

Java(TM) Plug-in will be used as the default Java Runtime in the following browser(s):

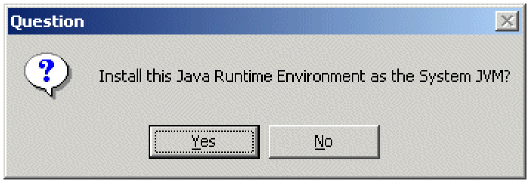
□ Microsoft Internet Explorer

☑ Netscape 6

Figure 5-27 Browser tab of Java Plug-in control panel, IBM 1.4 for Win32

For more information about the Java Plug-in control panel, see “The Java 2 Plug-in control panel” on page 221.

However, there is a message box that appears during the installation of this IBM Java 2 plug-in that might lead you to think that it is offering an option to set the Java 2 plug-in as the default JVM for Internet Explorer at installation time. The message box is shown in Figure 5-28.


Question

Install this Java Runtime Environment as the System JVM?

Figure 5-28 Message box during installation of IBM Java 2 plug-in runtime

In fact, the effect of clicking **Yes** on this panel is to copy the Java 2 versions of java.exe and javaw.exe to \winnt\system32. Your users may select either **Yes** or **No**. This will not affect the setting of Internet Explorer's default JVM.

5.17 The Java 2 plug-in

IBM recommends that you use an IBM Java 2 plug-in to run Host On-Demand if an IBM Java 2 plug-in is available for the platform.

5.17.1 Java 2 plug-ins supported

Host On-Demand currently supports the following Java 2 Plug-ins.

Table 5-15 Java 2 plug-ins supported

Vendor	Version
IBM	1.3.1, 1.4.0, 1.4.1
Sun	1.3.1, 1.4.0, 1.4.1
HP	1.3.1, 1.4.0, 1.4.1

New Java 2 plug-ins

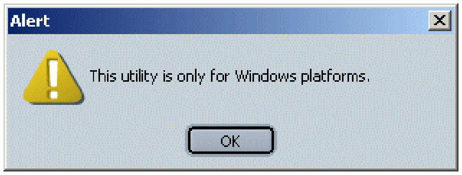
When Host On-Demand has been tested with later versions of the Java 2 plug-in, the news will be posted on the Host On-Demand Web site.

5.17.2 Clients can download Java 2 runtime for Win32 platform

Host On-Demand, for all platforms, includes an install image of the IBM Java 2 plug-in version 1.4.0 (build 20030614) runtime for the Win32 platform. Therefore, any client running on a Win32 platform can attach to a Host On-Demand server, (no matter what platform the server is running on), downloads this install image, and installs the Java 2 runtime for Win32 clients.

To download this installable version of the IBM Java 2 plug-in, the user should connect to `HODMain.html` and click **IBM 32-bit Runtime Environment for Java 2.**

If the client is running on a non-Win32 platform and this option is selected, the following message is displayed in Figure 5-29.



This utility is only for Windows platforms.

Figure 5-29 Attempt on non-Win32 platform to download Java 2 runtime for Win32

Do not use this plug-in for Win95 clients. Instead, download the Win95-compatible plug-in from the WebSphere Host On-Demand Web page:

`http://www-3.ibm.com/software/webservers/hostondemand/support.html`

Installing the plug-in on the Win32 platform

See “However, there is a message box that appears during the installation of this IBM Java 2 plug-in that might lead you to think that it is offering an option to set the Java 2 plug-in as the default JVM for Internet Explorer at installation time. The message box is shown in Figure 5-28.” on page 217 for a discussion of one of the install panels for the IBM Java 2 plug-in version 1.3.1 runtime.

A restricted user will not be allowed to install the plug-in.

Java plug-in for non-Win32 clients

For information on acquiring a Java 2 plug-in for a non-Win32 client, see the online document *Planning, Installation, and Configuration Guide for Host On-Demand*.

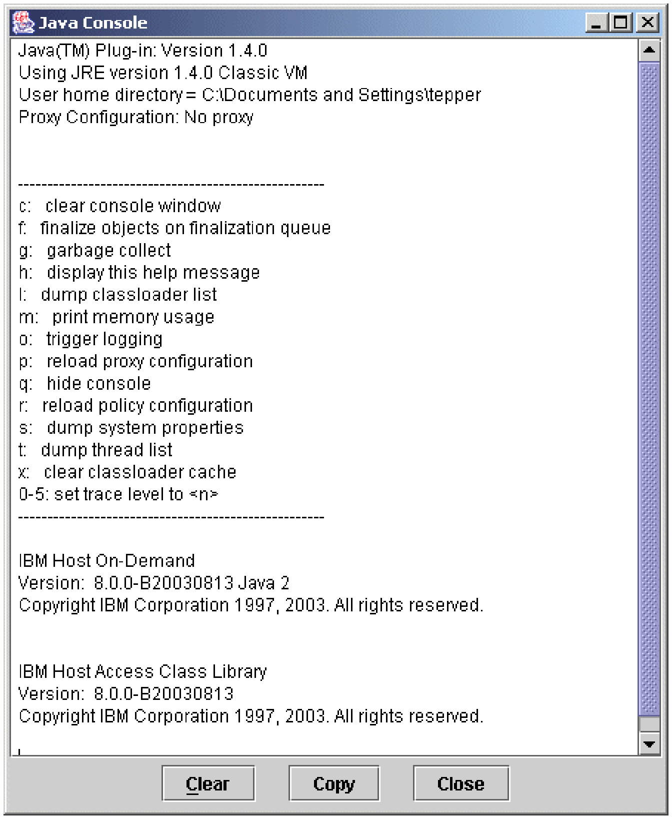
Warning against having multiple Java 2 plug-ins installed

In our experience having multiple Java 2 plug-ins causes problems. If you have multiple Java 2 plug-ins installed, then:

- Uninstall all the Java 2 plug-ins.
- Install the Java 2 plug-in that you want to use.

The Java 2 Java Console

Figure 5-20 shows the Java 2 Java Console.



```
Java(TM) Plug-in: Version 1.4.0
Using JRE version 1.4.0 Classic VM
User home directory = C:\Documents and Settings\tepper
Proxy Configuration: No proxy


----------------------------------------------------
c:   clear console window
f:   finalize objects on finalization queue
g:   garbage collect
h:   display this help message
l:   dump classloader list
m:   print memory usage
o:   trigger logging
p:   reload proxy configuration
q:   hide console
r:   reload policy configuration
s:   dump system properties
t:   dump thread list
x:   clear classloader cache
0-5: set trace level to <n>
----------------------------------------------------


IBM Host On-Demand
Version:  8.0.0-B20030813 Java 2
Copyright IBM Corporation 1997, 2003. All rights reserved.


IBM Host Access Class Library
Version:  8.0.0-B20030813
Copyright IBM Corporation 1997, 2003. All rights reserved.
```

Figure 5-30   Java 2 console

Do not allow the console to appear immediately

The Java Console can be set to appear either as soon as the JVM is started, or at a later time. With Host On-Demand you should set the Java Console to appear later. Otherwise, problems can occur with Host On-Demand's Java 2 detection.

Having the Java Console appear later will not cause you to lose any debug output or error messages. After you make the Java Console appear, scroll the window back to view any debug output or error messages that have occurred.

To stop the Java Console from appearing immediately, set the appropriate option on the Basic tab of the Java Plug-in control panel. See "The Java 2 Plug-in control panel" on page 221.

To make the Java Console appear later:

- On Win32 platforms, wait until the Host On-Demand desktop panel appears, then click the Java 2 icon in the plug-in section of the Windows taskbar. The icon will be a small version of either the Java coffee cup icon or the Duke (gnome) icon.

- On non-Win32 platforms, wait until the Host On-Demand desktop panel appears, then look for the icon in the system tray. If you do not find it, consult the Java 2 Plug-in documentation.

The figure below shows enlarged images of the Java coffee cup icon and the Duke (gnome) icon for popping up the Java console on the Win32 platform.

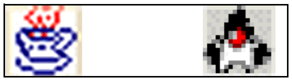


Figure 5-31 Icons for popping up Java 2 Java console on the Win32 platform

Using the console to determine vendor and version

To determine the vendor and version of the Java 2 Plug-in being run, pop up the Java 2 console and type the letter `s`. This causes the system information to be dumped to the console.

Scroll back through the system information and find the following three entries: java.vendor, java.version, and java.vm.info.

Here is the information for these entries when the Java 2 Plug-in is the version 1.4.0 runtime for the Win32 platform. The install image for this runtime is distributed with Host On-Demand and is downloadable by Win32 Host On-Demand clients no matter what platform the Host On-Demand server is running on:

```
java.vendor=IBM Corporation

java.version=1.4.0

java.vm.info = J2RE 1.4.0 IBM Windows 32 build cn1401-20030614 (JIT
enabled: jitc)
```

The Java 2 Plug-in control panel

The Java 2 plug-in includes a Java Plug-in control panel for configuring the plug-in.

Starting the control panel

The following table shows how to start the control panel on the Win32 and Linux platforms. For other platforms, consult the documentation distributed with the plug-in.

Table 5-16 How to start the Java 2 Plug-in control panel

Platform:	Plug-in Access
Win32	- IBM Java 2 1.4.0 plug-in Click Start, Programs, Java Plug-in control panel, or Click the icon on the desktop - Sun Java 2 1.4.0 plug-in Click Start, Settings, control panel, Java Plug-in, or Click the icon on the desktop
Linux	- IBM Java 2 1.4.0 <install>/jre/bin/JavaPluginControlPanel - Sun 1.4.0 <install>/jre/bin/ControlPanel

For Win32, the icon will be either a Java coffee cup icon or a Duke (gnome) icon. Figure 5-32 shows an enlarged image of the Java coffee cup icon on the Win32 desktop for launching the Java 2 Plug-in control panel.

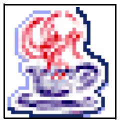
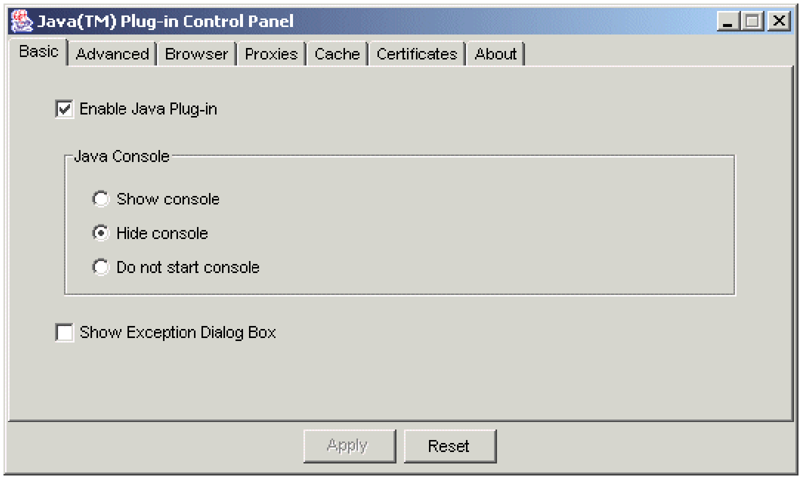


Figure 5-32 Icon for launching the Java 2 Plug-in control panel from Win32 desktop

Control panel settings, IBM plug-in 1.4.0 for Win32 platform

Figure 5-33 shows the Java Plug-in control panel for the IBM Java 2 Plug-in version 1.4.0. The install image for the runtime of this version of the plug-in is distributed with Host On-Demand, and is downloadable by Win32 Host On-Demand clients no matter what platform the Host On-Demand server is running on.

.



☑ Enable Java Plug-in

Java Console

○ Show console

● Hide console

○ Do not start console

□ Show Exception Dialog Box

Figure 5-33 Java Plug-in control panel for IBM Plug-in 1.4.0 for Win32

The recommended settings for each tab are as follows:

- Basic tab
  - Enable Java Plug-in.

    Check this checkbox.
  - Show Java console

    Causes the Java console to be displayed as soon as the JVM is started. Do not check this checkbox. See “Do not allow the console to appear immediately” on page 220.
  - Show Exception Dialog Box

    Causes a popup window to appear if an exception occurs. Do not check this checkbox.
- Advanced tab
  - Java Runtime Environment

    Enables the user to switch between several installed Java 2 Plug-ins. Leave this set to the first setting `Use Java Plug-in Default`.
  - Enable Just In Time Compiler

    Select this checkbox.
  - Java runtime parameters

    Additional runtime parameters are to be set when the JVM is started. Leave it blank.

- Proxies tab
  - Use browser settings

    When this checkbox is checked, it causes the Java 2 plug-in to read and use the browser's proxy settings. When not checked, it causes the Java 2 plug-in to use the proxy settings set on this panel.

    Normally, this checkbox should be checked; that is, the plug-in should use the browser's proxy settings.

    However, sometimes the plug-in cannot read the browser's proxy settings. This may cause a situation in which the Host On-Demand session cannot connect to the Host On-Demand server, even though the browser can connect to the Host On-Demand server. In this situation, deselect this checkbox and try filling in the browser's proxy settings on this panel.
  - Proxy settings

    See the preceding item.
- Cache tab

  This button clears the sticky cache. HOD does not use the sticky cache any longer.
- Certificates tab

  This tab displays the certificates that the user has granted *always* while running a Web browser, and allows the user to revoke the acceptance by deleting the certificate.

Settings for Sun Java 2 plug-in 1.3.1 for Win32 platform

The Java Plug-in control panel for the Sun Java 2 Plug-in Version 1.4.0 is similar to the control panel for the IBM Java 2 Plug-in Version 1.4.0. See the preceding section.

Additional settings for Sun Java 2 plug-in 1.4 for Win32 platform

This section describes the settings for which the Java Plug-in control panel for Sun Java 2 Plug-in 1.4 is different from the IBM Java 2 Plug-in 1.4.

- Basic tab
  - Show console, Hide console, or Do not start console.

    If set to `Show` or `Hide`, this causes problems for the Host On-Demand browser detection on Win32 platforms. See "Do not allow the console to appear immediately" on page 220. Set to `Do not start console`.

  - Show Java in System Tray

    Controls whether an icon is displayed for the Java console in the plug-in area of the Windows task bar when the JVM is started.

    Select this checkbox.

- Browser tab

  Controls whether the Java 2 plug-in functions as the default JVM for Internet Explorer and Netscape 6.

  For the checkbox for Internet Explorer, IBM recommends that you do not check the checkbox. See “Default JVM for Internet Explorer must be MS Java 1 JVM” on page 216.

  For the checkbox for Netscape 6, check the checkbox. See “Default JVM for Internet Explorer must be MS Java 1 JVM” on page 216.

- Cache tab

  The View button lets you view the names of the modules in the cache and selectively delete modules.

5.18 Additional information

Installing Netscape 6.x on the Win32 platform

First, see the warning in 5.17, “The Java 2 plug-in” on page 218 against having multiple Java 2 plug-ins installed.

Second, decide whether on the Win32 platform you want to run Netscape 6.X with the Sun Java 2 Plug-in or with the IBM Java 2 Plug-in.

Note: IBM recommends that you use the IBM Java 2 Plug-in with Host On-Demand.

If you want to run Netscape 6.x with the Sun plug-in, install the Sun plug-in as part of the Netscape 6.x install. In the directions below, choose **Full** or **Custom**. If you want to run Netscape 6.x with the IBM plug-in, do not install the Sun plug-in as part of the Netscape 6.x install. In the directions below, choose **Recommended** or **Custom**.

The Netscape 6.x install program has three main options:

- Recommended

  This option does *not* install the Sun Java 2 plug-in.

- Full

  This option installs the Sun Java 2 plug-in as part of the Netscape 6.x install.

- Custom

  On the Additional Options panel, check the **Sun Java 2** checkbox if you want to install the Sun Java 2 plug-in as part of the Netscape 6.x install. Do not check the Sun Java 2 checkbox if you plan to install the IBM Java 2 plug-in.

Sometimes Netscape 6.x on the Win32 platform has trouble finding the IBM Java 2 plug-in if the plug-in is installed first. If Netscape 6.x cannot find the Java 2 plug-in, follow these steps:

1. Uninstall any Java 2 plug-ins that are installed.
2. Install Netscape 6.x without the Sun Java Plug-in.
3. Install the IBM Java 2 plug-in.

Unexpected result with Internet Explorer

The fact that Internet Explorer has access both to its own internal Java 1 JVM and to a Java 2 JVM through the Java 2 plug-in can occasionally lead to an unexpected result.

For example, consider the following scenario on the client:

- The browser is Internet Explorer.
- The client is a cached client.
- The client Java type in the HTML file is Java 1.
- The Java 2 plug-in is installed.

Because the Java 2 plug-in is installed, you might expect that Host On-Demand would refuse to run the Java 1 cached client. That is exactly what happens if you try this scenario on Netscape 6.x with the Java 2 plug-in. See 5.12.4, “Startup behavior for Java 1 cached client” on page 197.

However, in this case, because Internet Explorer has access to its default JVM, and because Host On-Demand assumes that the default JVM is set to the Microsoft Java 1 JVM, therefore, Host On-Demand goes ahead and launches the Java 1 Host On-Demand cached client on the default JVM. See 5.12.4, “Startup behavior for Java 1 cached client” on page 197.

Microsoft JVM level for Internet Explorer

For Internet Explorer, the current version (or build number) of the Microsoft virtual machine (Microsoft VM) is 3810. You can update previous versions of the Microsoft VM to Build 3810 if you install the 816093 critical update.

Attention: Microsoft recommends to install this critical update due to a security lack.

For additional information about how to obtain and install the 816093 critical update, click the following article number to view the article in the Microsoft Knowledge Base:

```
http://support.microsoft.com/default.aspx?scid=kb;EN-US;816093"816093
MS03-011: Flaw in the Microsoft VM Could Enable System Compromise
```

Customers can raise this required level for Host On-Demand by using the following session parameter:

```
<PARAMETER NAME=JVM_Minimum  VALUE=xxxx>
```

An easy way to add this parameter is to use the Deployment Wizard, Additional Options page, Advanced Options panel, and Additional Parameters tab.

Note: The Microsoft JVM is Java 1. Customers using Java 1 cannot take advantage of the various new features in Host On-Demand. IBM encourages you to migrate to Java 2.

5.18.1 More information on the new Java 2 cache

Java 2 has three options for caching the files needed by an applet:

- No caching, that is, download the files each time the applet is run.
- Browser caching. This is the default.
- Plug-in caching

Host On-Demand's Java 2 download client still uses the default setting, browser caching. The Java 2 cached client up to Host On-Demand Version 7 used the sticky cache for plug-in caching. This caused several limitations. To be able to incorporate the new functions as described in 5.9.3, “Improvements to the cached client for Java 2” on page 181, the cached client had to be redesigned.

Instead of using the sticky cache, Host On-Demand Version 8’ s Java 2 cached client now uses its own cache, making Java 2 caching more like the methodology used in Java 1.

Attention: The HODAdmin Cached clients and the Java 2 Cached client on MAC still use the sticky cache.

The location where the cached archives will be stored will be determined by Java 2's user.home property (using only that portion up to and including the username), along with the hostname of the Web page visited. A "HODCC" is added to the hostname to prevent a "funny-looking" directory if the user specifies a dotted decimal (for example, 9.27.63.12), IP address, and then either "Debug" or "Release" depending on if the administrator has chosen to use Problem Determination components in the DW. So for example, if the client (user name harry) visited a Web site called:

```
http://www.midi.com/hod/HODCached.html
```

the local directory where the cached client is stored is (for Windows XP or Windows 2000):

```
C:\Documents and Settings\harry\HODCCwww.midi.com\Release
```

When a user points to this HTML page again (for example, from the same Web server), the code will again look at the user.home property, then add the "HODCCwww.midi.com" and then "Release" and see that the cached client is already installed.

To be able to support multi-user Windows systems like Windows 2000 and WIndows XP, two additional parameters have been added:

- ShareCachedClient
- SharedCachedDirectory

These are described in "Sharing the Host On-Demand Java 2 cached client" on page 154.

Here is a summary of the locations where the cached client will be stored.

- If no parameters are specified, then it will go in:

  ```
  c:\Documents and Settings\harry\HODCCwww.midi.com\Release
  ```

- If ShareCachedClient is set to true, but the location is not specified, then it will go in:

  ```
  c:\Documents and Settings\All Users\HODCCwww.midi.com\Release
  ```

- If ShareCachedClient and the store location are specified, then it will go in:

  ```
  \storelocation\HODCCwww.midi.com\Release
  ```

Note: The SharedCachedDirectory parameter, which allows an administrator to specify the directory location is ignored unless the ShareCachedClient = true is also set.

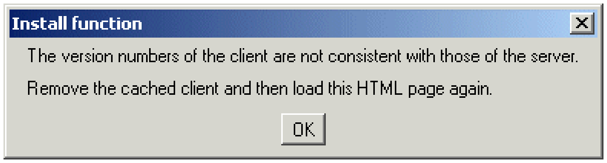
If the SharedCachedClient parameter = true, a .LOC file will point to the directory where the cached client is stored. This file is used when removing the cached client.

5.18.2 More information on the cached client

Scenario requiring Java 1 cached client to be removed

Here is an example of an upgrade scenario that requires the Java 1 cached client be removed.

- The user attaches to server HODSRV1, which is running a particular level of code, say HOD8. The user runs an HTML file, which installs a Java 1 cached client with a preload list. At this point the components on the preload list are installed on the user's machine.
- The user attaches to a second server HODSRV2, which is running a lower level of code, say HOD7 GM. Even though the user is attached to a different server, no additional components are needed so far. The Java 1 cached client on the user's machine uses the components already installed from HODSRV1.
- Now the user tries to access a component that was not installed from server HODSRV1, because it was not on the preload list. In this scenario, Host On-Demand displays the message in Figure 5-34.



The version numbers of the client are not consistent with those of the server.

Remove the cached client and then load this HTML page again.

Figure 5-34 Version numbers not consistent

The problem is that the Java 1 components at the second server are older than the Java 1 components already downloaded by the cached client. Host On-Demand will not install an older Java 1 cached client over a newer one.

Therefore, in this scenario, the user has to remove the cached client, and then re-install the cached client at the second server.

5.18.3 More information on the download client

Reason for restriction on Java 1 download client

The reason that the Java 1 download client cannot be run while the Java 1 cached client is installed has to do with the order in which the Java 1 JVM for Internet Explorer looks for class files when the cached client is installed. Remember, in the following discussion, we are talking about the Java 1 cached client and the Java 1 download client, not the Java 2 cached client and download client. Also, we are talking about Internet Explorer not Netscape 4.x.

When the Java 1 cached client is installed and the user is running Internet Explorer, Host On-Demand includes at the first of the system classpath the path of the HODCC directory where the user's cached client class files are installed. Consequently, when a Host On-Demand Java method is called, the JVM looks in the HODCC directory before looking in the JAR files downloaded by the browser in the browser cache.

Now suppose that the Java 1 download client is run without the Java 1 cached client being installed. This is the normal case. When the download client is run and a Java method is called, the JVM first looks in the HODCC directory for the class file. The HODCC directory does not exist, because the cached client is not installed. Therefore, the JVM looks for, and finds, the class file in one of the Java 1 download client's JAR files in the browser cache.

Now suppose hypothetically that:

- The Java 1 cached client is installed and Host On-Demand allows the Java 1 download client to be run. (In fact, Host On-Demand does not allow this.)
- The cached client and the download client are different levels of Host On-Demand code, for example, version 7.0 and version 8.0.
- A function called MyMethod() has changed between version 7.0.0 and 7.0.1

When the Java 1 download client is run and MyMethod() is called, the JVM looks for the class file first, and finds it in the HODCC directory. Therefore, the JVM executes the Java 1 cached client version of MyMethod() instead of the download client version. Because the wrong version is executed in this situation, an error caneasily occur. The error can be minor or possibly catastrophic.

To avoid this scenario, the Java 1 version of Host On-Demand does not allow the download client to be run while the cached client is installed.

Reasons for three limitations on the Java 2 download client

The three minor limitations on the Java 2 download client that are described in 5.15, "The Java 2 download client" on page 212 are the result of two restrictions that affect the Java 2 download client:

- JAR/CAB file restriction

  For both the Java 1 and Java 2 download clients, all JAR or CAB files that are downloaded have to be specified in the **APPLET** command, which launches the download client.

  Unlike the cached client, the download client does not have a CachedAppletSupport applet to download JAR or CAB files after the client is launched.

  The Java 1 download client gets around this restriction by downloading components not on the preload list as loose class files rather than as JAR or CAB files.

- Signing restriction

  The Java 2 JVM requires that all modules belonging to the same Java package must be signed in the same way.

  This requirement means that the class files belonging to a Java package may be:

  – A collection of loose class files (unsigned)
  – A collection of class files in an unsigned JAR file
  – A collection of class files in one or more JAR files signed with the same certificate

  Likewise, the class files belonging to a Java package may *not* be:

  – A collection of JAR files signed with different certificates
  – A collection of signed JAR files and unsigned JAR files
  – A combination of a signed JAR file and loose class files (unsigned)

Now we can explain the limitations.

The reason for the first limitation described in 5.15, “The Java 2 download client” on page 212, that no component can be downloaded that is not on the preload list, is that after being launched the Java 2 download client is prevented from downloading additional components either as JAR or CAB files (because of the JAR/CAB file restriction described above) or as loose class files (because of the signing restriction described above). Therefore the Java 2 download client cannot download an additional component.

The reason for the second limitation, which is that the Function On-Demand client will not run correctly, is that the Function On-Demand client is a download client with a preload list. It contains a core of function that is intended to be augmented by components downloaded after the applet is launched. Therefore, this limitation is really a particular instance of the first limitation above.

The third limitation, which is that the default download clients do not contain some components, is yet another particular instance of the first limitation mentioned previously. In order to reduce the startup time of the default download clients, some components are omitted. Therefore, the default download clients are download clients with preload lists, and fall under the first limitation.

5.18.4 More information on launching the Host On-Demand applets

This section provides more information on how the Host On-Demand applets (the HostOnDemand applet and the CachedAppletSupport applet) are launched.

Download client on Java 1 browser

Example 5-3 shows how a Host On-Demand HTML file launches the download client on a Java 1 browser. The command is **APPLET** for both Internet Explorer and Netscape 4.77, and the parameters are exactly the same for Internet Explorer and Netscape 4.77.

Example 5-3 Download client on Java 1 browser

```
<APPLET
   ARCHIVE="habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hodsignn.jar,
            hamacrtn.jar,hacltaun.jar,hodhlln.jar, havtn.jar,haslpn.jar,
            hakeypdn.jar,ha3270n.jar,hamacuin.jar,hodmacn.jar,haprintn.jar,
            halumn.jar,ha3270xn.jar,hodcfgn.jar,sccbase.jar,ha5250xn.jar,
            hodssln.jar,ha3270pn.jar,hassln.jar,hacicsn.jar,haftpn.jar,
            ha5250pn.jar,hahostgn.jar,haxfern.jar,ha5250n.jar,hodappln.jar,
            hakeympn.jar,hacolorn.jar,hodimpn.jar,ha5250en.jar"
   NAME="HODApplet"
   CODE="com.ibm.eNetwork.HOD.HostOnDemand"
   WIDTH="80%"
   HEIGHT="80%">
<PARAM NAME="Cabinets"        VALUE="habasen.cab,hodbasen.cab,hodimg.cab,
                                     hacp.cab,hodsignn.cab,hamacrtn.cab,
                                     hacltaun.cab,hodhlln.cab,havtn.cab,
                                     haslpn.cab,hakeypdn.cab,ha3270n.cab,
                                     hamacuin.cab,hodmacn.cab,haprintn.cab,
                                     halumn.cab,ha3270xn.cab,hodcfgn.cab,
                                     sccbase.cab,ha5250xn.cab,hodssln.cab,
                                     ha3270pn.cab,hassln.cab,hacicsn.cab,
                                     haftpn.cab,ha5250pn.cab,hahostgn.cab,
                                     haxfern.cab,ha5250n.cab,hodappln.cab,
                                     hakeympn.cab,hacolorn.cab,hodimpn.cab,
                                     ha5250en.cab">
<PARAM NAME="ParameterFile"   VALUE="HODData\augj1dl\params.txt">
<PARAM NAME="JavaScriptAPI"   VALUE="false">
```

In Example 5-3, note that:

- In the first line the command is **APPLET**.
- In the ARCHIVE attribute JAR files are listed, while in the Cabinets parameter CAB files are listed. If the browser is Netscape, then the JAR files are downloaded; if the browser is Internet Explorer, then the CAB files are downloaded.
- In the ARCHIVE attribute and in the Cabinets parameter the modules are Java 1 modules. This is evident from the fact that the module names do not end with `2`. Examples: `habasen.jar` and `hodbasen.jar`.
- In the CODE parameter the class to be invoked is com.ibm.eNetwork.HOD.HostOnDemand. This is the entry point for the HostOnDemand applet.

Cached client on Java 1 browser

The example below shows how a Host On-Demand HTML file launches the cached client on a Java 1 browser. The command is **APPLET** for both Internet Explorer and Netscape 4.77, and the parameters are exactly the same for Internet Explorer and Netscape 4.77.

Although the cached client is invoked in two different circumstances, to install the cached client and to start the installed cached client, the applet is launched in the same way in both circumstances. The applet itself determines whether the cached client needs to be installed.

Example 5-4 Cached client on Java 1 browser

```
<APPLET
   ARCHIVE="CachedAppletSupporter.jar"
   MAYSCRIPT
   NAME="CachedAppletSupporter"
   CODE="com.ibm.eNetwork.HOD.cached.appletsupport.CachedAppletSupportApplet"
   WIDTH="2"
   HEIGHT="2">
<PARAM NAME="Cabinets"                VALUE="CachedAppletSupporter.cab">
<PARAM NAME="DebugComponents"         VALUE="false">
<PARAM NAME="PreloadComponentList"    VALUE="HABASE;HODBASE;HODIMG;HACP;
                                            HAFNTIB;HAFNTAP;HAMACRT;
                                            HACLTAU;HODHLL;HAVT;HASLP;
                                            HAKEYPD;HA3270;HAMACUI;
                                            HODMAC;HAPRINT;HALUM;HA3270X;
                                            HODCFG;SCCBASE;HA5250X;HODSSL;
                                            HA3270P;HASSL;HACICS;HAFTP;
                                            HA5250P;HAHOSTG;HAXFER;HA5250;
                                            HODAPPL;HAKEYMP;HACOLOR;
                                            HODIMP;HA5250E">
<PARAM NAME="DebugCachedClient"       VALUE="false">
```

```
<PARAM NAME="CachedClientSupportedApplet"
VALUE="com.ibm.eNetwork.HOD.HostOnDemand">
<PARAM NAME="InstallerFrameWidth"         VALUE="550">
<PARAM NAME="InstallerFrameHeight"        VALUE="250>"
<PARAM NAME="UpgradePromptResponse"       VALUE="Prompt">
<PARAM NAME="UpgradePercent"              VALUE="100">
</APPLET>
```

In the above example, note that:

- In the first line the command is **APPLET**.
- In the ARCHIVE attribute a JAR file is listed, while in the Cabinets parameter a CAB file is listed. If the browser is Netscape, then the JAR file is downloaded; if the browser is Internet Explorer, then the CAB file is downloaded.
- In the ARCHIVE attribute and in the Cabinets parameter the modules are Java 1 modules. This is evident from the fact that the module names do not end with 2. Examples: CachedAppletSupporter.jar, CachedAppletSupporter.cab.
- In the CODE parameter the class to be invoked is com.ibm.eNetwork.HOD.cached.appletSupport.CachedAppletSupportApplet. This is the entry point for the CachedAppletSupport applet.
- The PreloadComponentList contains a list of the components that are to be downloaded initially. These are component names, not module names. A component may consist of one or more modules.
- The DebugCachedClient parameter is set to false.
- The CachedClientSupportedApplet parameter specifies the name of the applet to be launched if the cached client is installed. This is the HostOnDemand applet.

Download client on Java 2 browser

The example below shows how a Host On-Demand HTML file launches the Java 2 download client on Internet Explorer with the Java 2 plug-in. The command is **OBJECT**. On Netscape 6.x the command is **APPLET**, but the other information is almost exactly the same.

Example 5-5 Download client on Java 2 browser

```
<OBJECT
   classid="clsid:8AD9C840-044E-11D1-B3E9-00805F499D93"
   WIDTH=80%
   HEIGHT=80%
   ID="HODApplet">
<PARAM NAME=CODE VALUE="com.ibm.eNetwork.HOD.HostOnDemand">
```

```
<PARAM NAME=ARCHIVE VALUE = "habasen2.jar,hodbasen2.jar,hodimg.jar,
                            hacp.jar,hamacrtn2.jar,hacltaun2.jar,
                            hodhlln2.jar,havtn2.jar,haslpn2.jar,
                            hakeypdn2.jar,ha3270n2.jar,hamacuin2.jar,
                            hodmacn2.jar,haprintn2.jar,halumn2.jar,
                            ha3270xn2.jar,hodcfgn2.jar,sccbase2.jar,
                            ha5250xn2.jar,hodssln2.jar,ha3270pn2.jar,
                            hassln2.jar,hacicsn2.jar,haftpn2.jar,
                            ha5250pn2.jar,hahostgn2.jar,haxfern2.jar,
                            ha5250n2.jar,hodappln2.jar,hakeympn2.jar,
                            hacolorn2.jar,hodimpn2.jar,ha5250en2.jar">
<PARAM NAME="type" VALUE="application/x-java-applet;version=1.3">
<PARAM NAME="MAYSCRIPT"      VALUE="true">
<PARAM NAME="scriptable"     VALUE="true">
<PARAM NAME=RealDocumentBase
                      VALUE=http://localhost/hod/augj2dl.html?JavaType=java2>
<PARAM NAME="ParameterFile" VALUE="HODData\augj2dl\params.txt">
<PARAM NAME="ShowDocument"  VALUE="_parent">
<PARAM NAME="JavaScriptAPI" VALUE="false">
<PARAM NAME="PreloadComponentList" VALUE="HABASE;HODBASE;HODIMG;HACP;HAFNTIB;
                                          HAFNTAP;HAMACRT;HACLTAU;HODHLL;
                                          HAVT;HASLP;HAKEYPD;HA3270;HAMACUI;
                                          HODMAC;HAPRINT;HALUM;HA3270X;
                                          HODCFG;SCCBASE;HA5250X;HODSSL;
                                          HA3270P;HASSL;HACICS;HAFTP;HA5250P;
                                          HAHOSTG;HAXFER;HA5250;HODAPPL;
                                          HAKEYMP;HACOLOR;HODIMP;HA5250E">
</OBJECT>
```

In Example 5-5, note that:

- In the first line the command is **OBJECT**.
- In the ARCHIVE parameter, JAR files are listed. There is no Cabinets parameter, because the Java 2 plug-in uses JAR files.
- In the ARCHIVE parameter the modules are Java 2 modules. This is evident from the fact that the module names end in 2. Examples: habasen2.jar and hodbasen2.jar.
- In the CODE parameter the class to be invoked is com.ibm.eNetwork.HOD.HostOnDemand. This is the entry point for the HostOnDemand applet.
- The PreloadComponentList contains a list of the components that are to be downloaded initially. These are component names, not module names. A component may consist of one or more modules.

Cached client on Java 2 browser

The example below shows how a Host On-Demand HTML file launches the Java 2 cached client on Internet Explorer with the Java 2 plug-in. The command is **OBJECT**. On Netscape 6.x the command is **APPLET**, but the other information is almost exactly the same.

Example 5-6 Cached client on Java 2 browser

```
<HTML>
<!-- HOD WIZARD HTML -->
<!-- Deployment Wizard Build : 8.0.0-B20030813 -->
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<TITLE>cached_achim</TITLE>
<SCRIPT LANGUAGE="JavaScript" SRC="CommonJars.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="HODJavaDetect.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="CommonParms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript">

//---- Start JavaScript variable declarations ----//
var hod_Locale = '';
var hod_jsapi=false;
var hod_AppName ='';
var hod_AppHgt = '80%';
var hod_AppWid = '80%';
var hod_CodeBase = '';
var hod_FinalFile = 'z_cached.html';
var hod_JavaType = 'java2';
var hod_Obplet = '';
var hod_Comps = 'HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HAMACRT;HAKEYPD;
HA3270;HAMACUI;HODMAC;HODCFG;HODTLBR;HODAPPL;HAKEYMP;HACOLOR;HODIMP';
var hod_Archs = '';
var hod_Verss = '';

var hod_URL = new String(window.location);
var hod_DebugOn = false;
var hod_SearchArg = window.location.search.substring(1);

// put cached client installation applet parameters here
var cHod_AppletParams = new Array;
<PARAM NAME="DebugCachedClient"          VALUE="false">';
c<PARAM NAME="DebugComponents"            VALUE="false">';
<PARAM NAME="UpgradePromptResponse"      VALUE="Prompt">';
<PARAM NAME="UpgradePercent"             VALUE="100">';
<PARAM NAME="InstallerFrameWidth"        VALUE="550">';
<PARAM NAME="InstallerFrameHeight"       VALUE="250">';
<PARAM NAME="JavaScriptAPI"              VALUE="' + hod_jsapi + '">';
<PARAM NAME="ConfiguredJavaType"         VALUE="' + hod_JavaType + '">';
```

```
// put Host On-Demand applet parameters here
var hHod_AppletParams = new Array;
<PARAM NAME="ShowDocument"               VALUE="_parent">';
<PARAM NAME="CachedClient"               VALUE="true">';
<PARAM NAME="DebugCachedClient"          VALUE="false">';
<PARAM NAME="ParameterFile"              VALUE="HODData\\cached\\params.txt">';
<PARAM NAME="JavaScriptAPI"              VALUE="' + hod_jsapi + '">';
//hHod_AppletParams[x] = '<PARAM NAME="DebugCode"      VALUE="65535">';

//---- End JavaScript variable declarations ----//

function getHODMsg(msgNum) {
  return HODFrame.hodMsgs[msgNum];
}

function getHODFrame() {
  return HODFrame;
}

var lang = detectLanguage(hod_Locale);
document.writeln('<FRAMESET cols="*,10" border=0 FRAMEBORDER="0">');

if (isMac()) {
  document.writeln('<FRAME  src="cached_J2.html" name="HODFrame">');
} else {
  document.writeln('<FRAME  src="hoddetect_' + lang + '.html"
name="HODFrame">');
}
document.writeln('</FRAMESET>');

</SCRIPT>
</HEAD>
</HTML>
```

In Example 5-6, note that:

- In the first line the command is **OBJECT**.
- In the CODE parameter, the class to be invoked is com.ibm.eNetwork.HOD.cached.appletLoader.CachedAppletLoader.class This is the entry point for the Java 2 CachedAppletSupport applet.
- The PreloadComponentList parameter contains a list of the components that are to be downloaded initially. These are component names, not module names. A component may consist of one or more modules.
- The cache_archive parameter lists the JAR files that are to be placed in the sticky cache. Host On-Demand specifies that all the JAR files should be placed in the sticky cache

- The cache_version parameter is a Host On-Demand parameter that tells the Cached Applet Support applet the versions of the modules in the sticky cache.
- In the ARCHIVE parameter the modules are Java 2 modules. This is evident from the fact that the module names end in `2`. Examples: `habasen2.jar`, `hodbasen2.jar`.
- The AppName parameter specifies the name of the applet to be launched if the cached client is installed. This is the HostOnDemand applet.
- The DebugCachedClient parameter is set to `false`.

6

Database On-Demand

In this chapter, we discuss the administration and client side of Database On-Demand. Database On-Demand is a Java applet that allows users to perform Structured Query Language (SQL) requests to iSeries databases through a Java Database Connectivity (JDBC) driver. Though Database On-Demand is shipped with a JDBC driver, other user-installed JDBC drivers can also be registered and used, although Host On-Demand does not provide support for other drivers.

6.1 Administering Database On-Demand

The first important point to understand is that an administrator cannot create SQL statements for users. One, however, can create groups and users, define the database functions that users can perform, manage statements that users have created, and create groups and users.

The Database On-Demand users are based on the users and groups that are defined in Host On-Demand, with the Database On-Demand being one attribute of this.

For example, let us say that two people in your organization will need to use Database On-Demand for SQL queries to an iSeries. Follow the directions below to configure these users for Database On-Demand.

6.1.1 Creating Database On-Demand groups and users

Use the Host On-Demand administration utility to create a group called DatabaseAdmin and the two users called “Greg and Kelly.” Make each user a member of the DatabaseAdmin group. The group name is not important, and can be anything that would best describe the group.

6.1.2 Configuring database options

In the Host On-Demand administration utility, right-click the **Database group** and click **Database -> Options...** (Figure 6-1 on page 241) and the Database On-Demand Group Options window (Figure 6-2 on page 242) will be displayed. Some options allow or restrict certain functions, while other options set default values. Database On-Demand provides the following two methodologies for granting users authority for options:

- Most permissive

  If a user belongs to two or more groups, the most permissive authority is granted for that option.

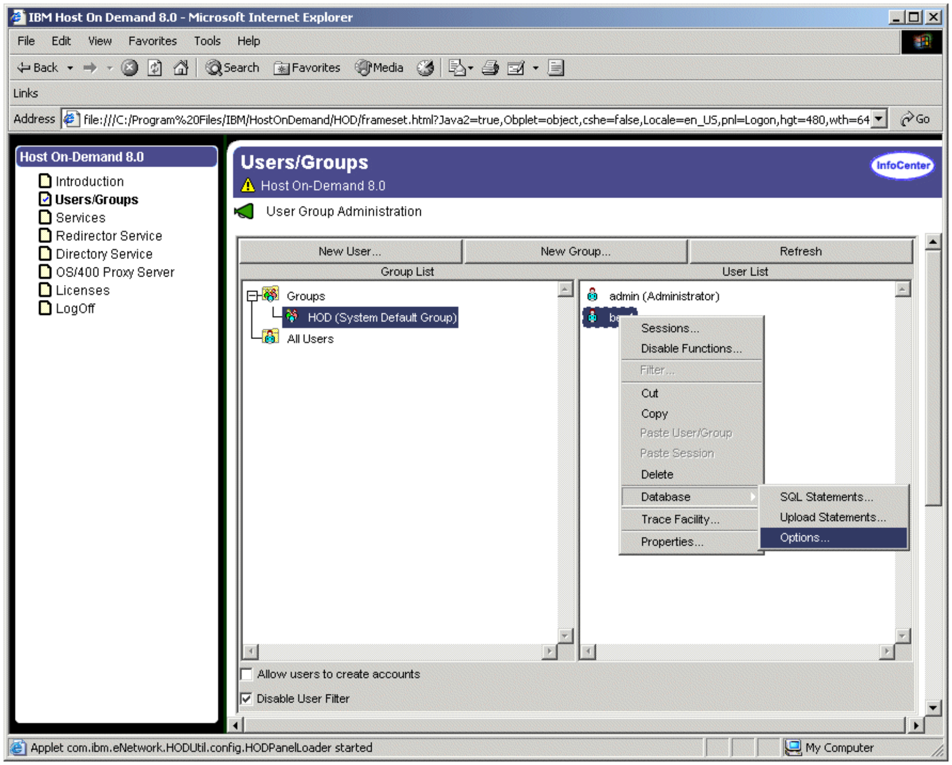
  For example, if a user is a member of DatabaseAdmin and this group allows deleting SQL statements, and the user is also a member of DatabaseUsers, but DatabaseUsers does not allow deleting SQL statements, the user is allowed to delete SQL statements.

- User override

  When options are modified for a selected user, the new settings override settings for the group or groups to which the user may belong. Default user options (those not explicitly set by a user or administrator) do not override group settings. This gives the administrator the ability to allow or restrict certain functions at the user level.

  For example, suppose a user belongs to DatabaseAdmin, which allows edit SQL statements, and the user level options do not allow edit SQL statements. The user cannot edit SQL statements, even though the DatabaseAdmin group allows it.

The Host On-Demand online help provides a table indicating how user authority for Database On-Demand is granted.



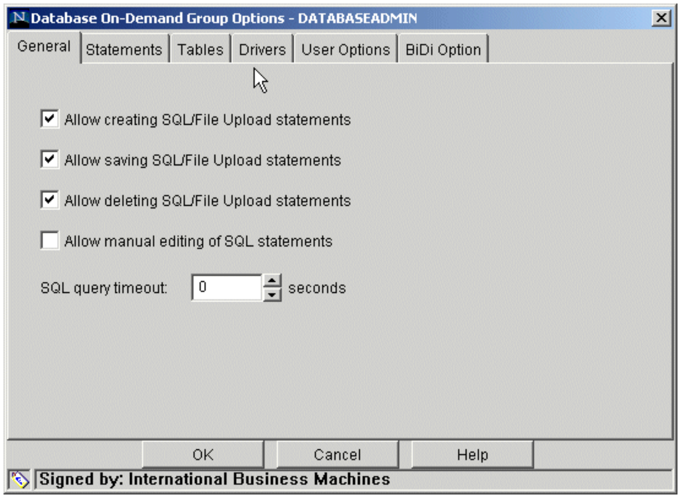
Address: file:///C:/Program%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=64

□ Allow users to create accounts

☑ Disable User Filter

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 6-1 Opening the Database On-Demand administrator window



Database On-Demand Group Options - DATABASEADMIN
General
Statements
Tables
Drivers
User Options
BiDi Option
OK
Cancel
Help
Signed by: International Business Machines

☑ Allow creating SQL/File Upload statements

☑ Allow saving SQL/File Upload statements

☑ Allow deleting SQL/File Upload statements

□ Allow manual editing of SQL statements

SQL query timeout: 0 seconds

Figure 6-2 Database On-Demand Group Options window

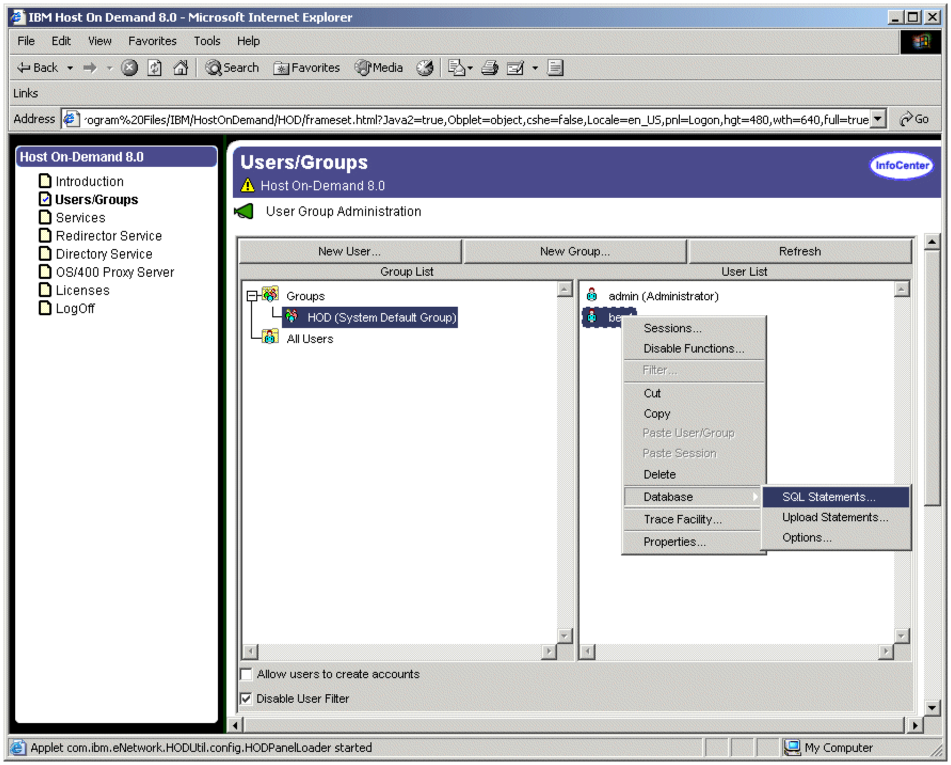
The configurable options available from this window are self explanatory, and more information is available in the Host On-Demand online help if required.

6.1.3 Administering SQL statements

Database On-Demand allows the administrator to manage SQL statements that were previously saved by a group or user; the administrator can copy, rename, or delete statements.

Let us say that Greg saved an SQL statement called List Employees and Kelly decides that access to the same database for the same information is useful. The administrator must complete these steps:

1. Right-click the user with the saved SQL statement (in the example, Greg), and click **Database -> SQL Statements...**. See Figure 6-3.



`ogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true`

□ Allow users to create accounts

☑ Disable User Filter

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 6-3 Preparing to copy a saved SQL statement from a user

2. When the Database On-Demand User Statements window is displayed as shown in Figure 6-4, select the saved SQL statement in the left-hand pane, in this example it is **List Employees**.
3. Select the user or group to which you wish to copy the SQL statement.

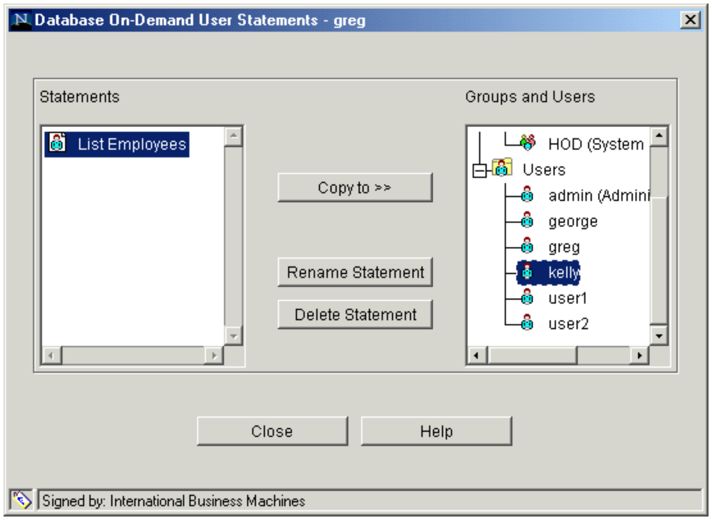
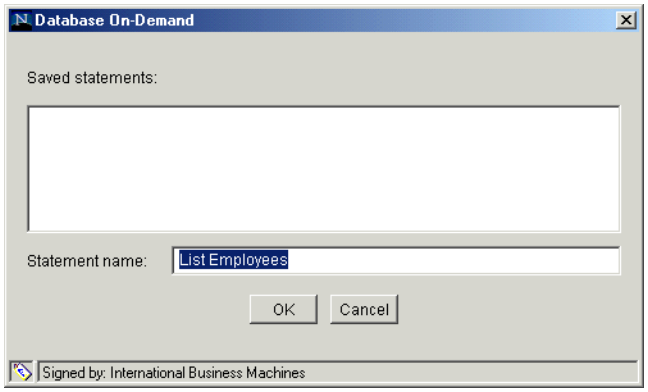


Figure 6-4 Copying saved SQL statements to a group

4. Click **Copy to >>** which will then show you any SQL statements already saved with that user, and provides an option of renaming the SQL if desired. See Figure 6-5.



Statement name: List Employees

Figure 6-5 Saving the SQL statement to another user

5. Click **OK** to save the SQL to that user ID.

6.2 Using Database On-Demand

Start Database On-Demand from HODMain.html or directly with HODDatabase.html, and log in. On the Database On-Demand applet window, as shown in Figure 6-6, you will see two tabs:

- SQL Wizard tab - The SQL Wizard is the default view. It displays a view of previously saved SQL statements.
- File Upload tab - This tab displays a view of previously saved File Upload statements.

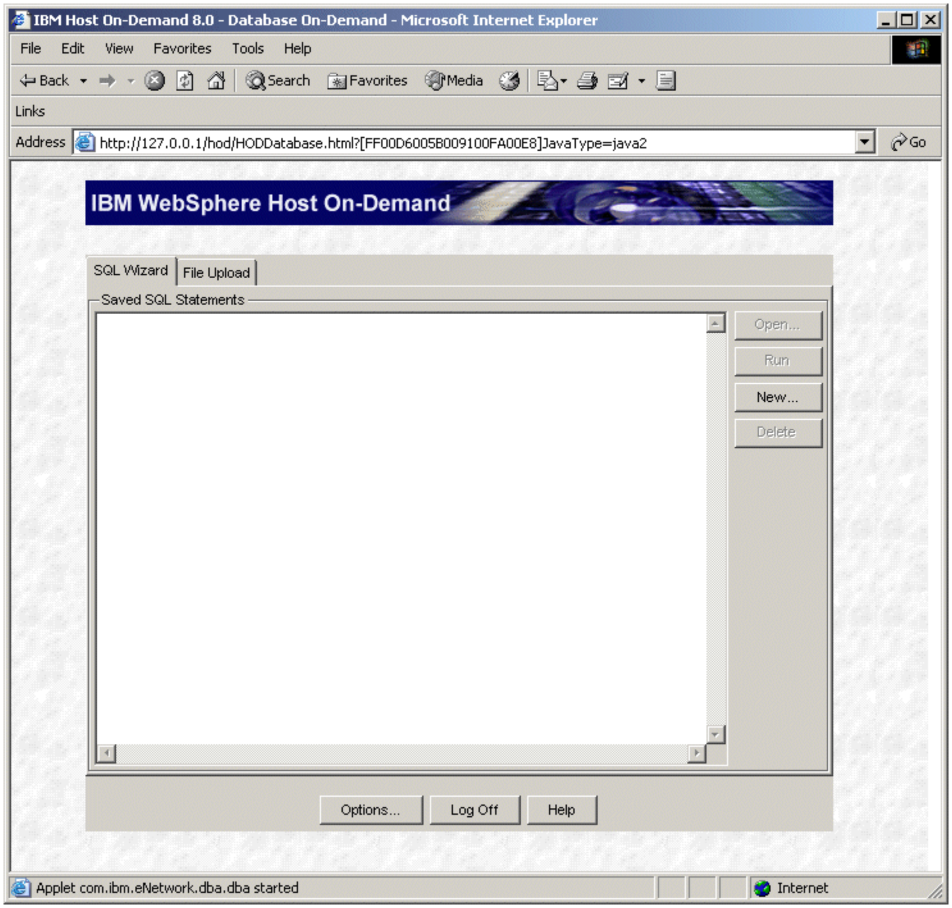

IBM Host On-Demand 8.0 - Database On-Demand - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Links
Address
http://127.0.0.1/hod/HODDatabase.html?[FF00D6005B009100FA00E8]JavaType=java2
Go
IBM WebSphere Host On-Demand
SQL Wizard
File Upload
Saved SQL Statements
Open...
Run
New...
Delete
Options...
Log Off
Help
Applet com.ibm.eNetwork.dba.dba started
Internet

Figure 6-6 Database On-Demand applet

From this applet, you can do the following:

- Create a new SQL or File Upload statement

- Run an existing SQL or File Upload statement
- Open an existing SQL or File Upload statement
- Delete an existing SQL or File Upload statement

6.2.1 Creating a new SQL statement

You can create a new SQL query by performing the following steps. By way of example, we create a query to list all the names of people at a certain zip code, using data stored in the Callup database hosted on an iSeries server.

Creating a new statement

From the Database On-Demand applet (Figure 6-6), perform these steps:

1. Click **New.**

   You are presented with the Logon window shown in Figure 6-7 on page 247.

2. Type the database URL:

   ```
   jdbc:as400://iSeriesname
   ```

   To use SSL when connecting, type:

   ```
   jdbc:as400://iSeriesname;secure=true
   ```

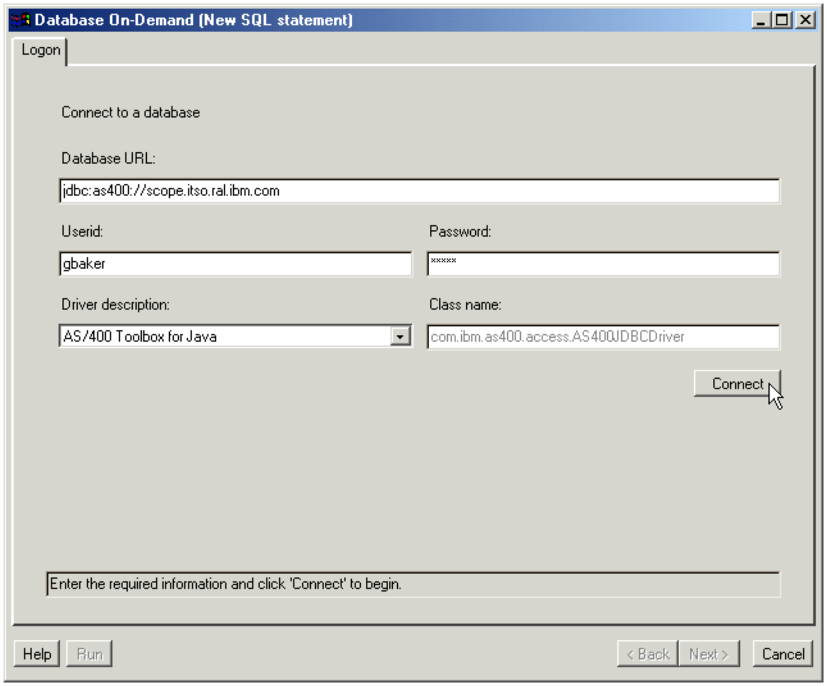
   To use the O/S400 Proxy Server without security:

   ```
   jdbc:as400://iSeriesname;proxy server=HODServername
   ```

   To use a secure connection via the OS/400 Proxy:

   ```
   jdbc:as400://iSeriesname;secure=true;proxy server=HODServername
   ```

3. Type your user ID and password (if required).
4. Select the JDBC driver you want to use to access the database. In this case, the driver supplied, called AS/400 Toolbox for Java, is used.
5. Click **Connect**.



Database On-Demand (New SQL statement)

Logon

Connect to a database

Database URL:
jdbc:as400://scope.itso.ral.ibm.com

Userid:
gbaker

Password:
*****

Driver description:
AS/400 Toolbox for Java

Class name:
com.ibm.as400.access.AS400JDBCDriver

Enter the required information and click 'Connect' to begin.

Figure 6-7 Database On-Demand Logon tab

When the connection to the iSeries has been made, the following tabs are added: Tables, Join, Condition 1, Columns, Sort, Output, SQL, and Results as shown in Figure 6-8.

Selecting a table

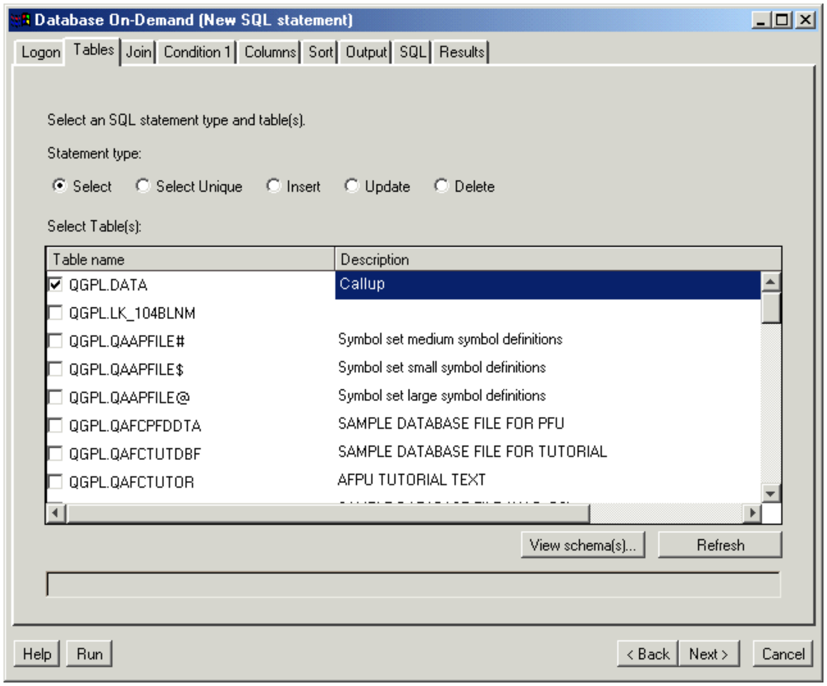
On the Tables tab there is a window in which to select tables from the host; also specify what type of SQL statement you want to use:

- Select
- Select Unique
- Insert
- Update
- Delete

You can select multiple tables when performing a select, or select unique.

In this example we chose the **Callup table** (QGPL.DATA):

1. Select the **QGPL.DATA** checkbox.
2. Since no join is required in this example, click **Condition 1** tab, or **Next** twice.



Select an SQL statement type and table(s).

Statement type:

● Select ○ Select Unique ○ Insert ○ Update ○ Delete

Select Table(s):

Table name	Description
☑ QGPL.DATA	Callup
□ QGPL.LK_104BLNM	
□ QGPL.QAAPFILE#	Symbol set medium symbol definitions
□ QGPL.QAAPFILE$	Symbol set small symbol definitions
□ QGPL.QAAPFILE@	Symbol set large symbol definitions
□ QGPL.QAFCPFDDTA	SAMPLE DATABASE FILE FOR PFU
□ QGPL.QAFCTUTDBF	SAMPLE DATABASE FILE FOR TUTORIAL
□ QGPL.QAFCTUTOR	AFPU TUTORIAL TEXT

Figure 6-8 Database On-Demand Tables tab

Selecting Conditions

We want to find all the people at a certain zip code, in this case 27709. On the Condition 1 window (Figure 6-9), the selected table should be displayed in the Selected table(s) field. If it is not, click the pull-down menu to select it.

1. Select **ZIP** in the Columns pane.

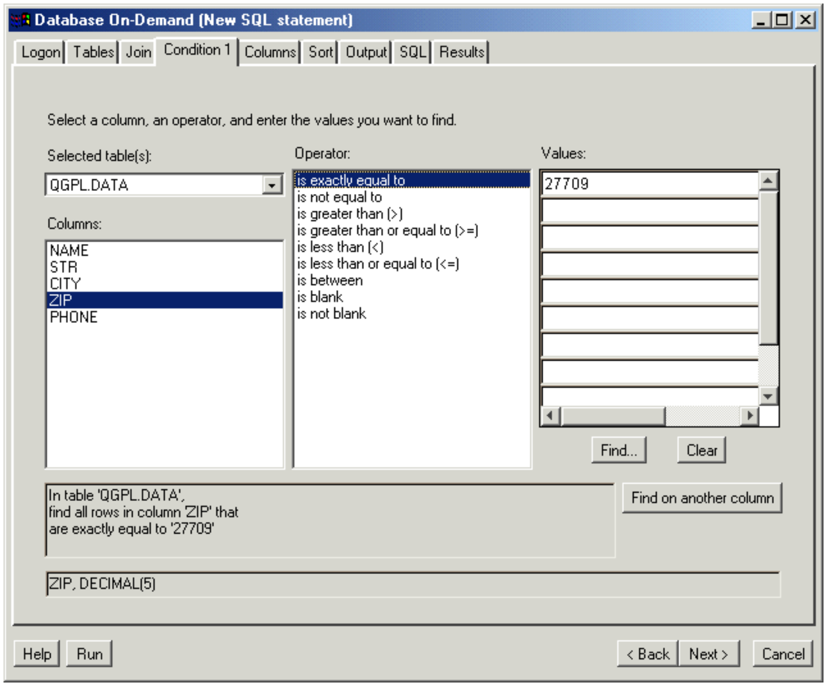
   You will see that it displays the field type and field length, such as ZIP and DECIMAL(5) towards the bottom of the window.

2. In the Operator pane, select **is exactly equal to**.
3. In the Values pane, enter `27709`.

   If required, you can see all the values for ZIP by clicking **Find...** and leaving the Search for field blank, and all the values for ZIP will be returned. You can select **27709** and click **Use values** to use that value.

4. Click **Next** or the **Columns** tab to continue.

If you have more than one selection criteria, you can add further conditions by clicking **Find** on another column. This will also add another Condition tab.



Select a column, an operator, and enter the values you want to find.

Selected table(s): QGPL.DATA

Columns: NAME, STR, CITY, ZIP, PHONE

Values: 27709

In table 'QGPL.DATA',
find all rows in column 'ZIP' that
are exactly equal to '27709'

ZIP, DECIMAL(5)

Figure 6-9 Database On-Demand Condition 1 tab

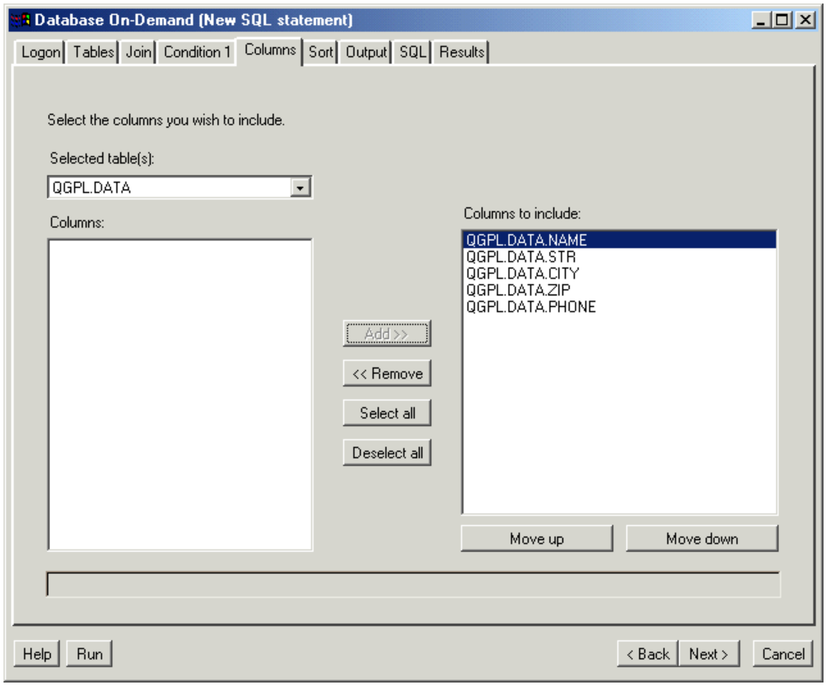
Selecting columns

The Columns window, shown in Figure 6-10, allows us to select which columns we want shown in the results. All available columns for the selected table, in this case QGPL.DATA, will be displayed in the left-hand pane labeled Columns. We want all columns displayed in the results, so we add them to the included columns by the following steps:

1. Click **Select all**.
2. Click **Add >>**.

   You can change the order that the columns are displayed in the results by selecting the included column in the right-hand pane, and either clicking **Move up** or **Move down** as desired.

3. Click **Next** or click the **Sort** tab to continue.



Select the columns you wish to include.

Selected table(s): QGPL.DATA

Columns:

Columns to include:
QGPL.DATA.NAME
QGPL.DATA.STR
QGPL.DATA.CITY
QGPL.DATA.ZIP
QGPL.DATA.PHONE

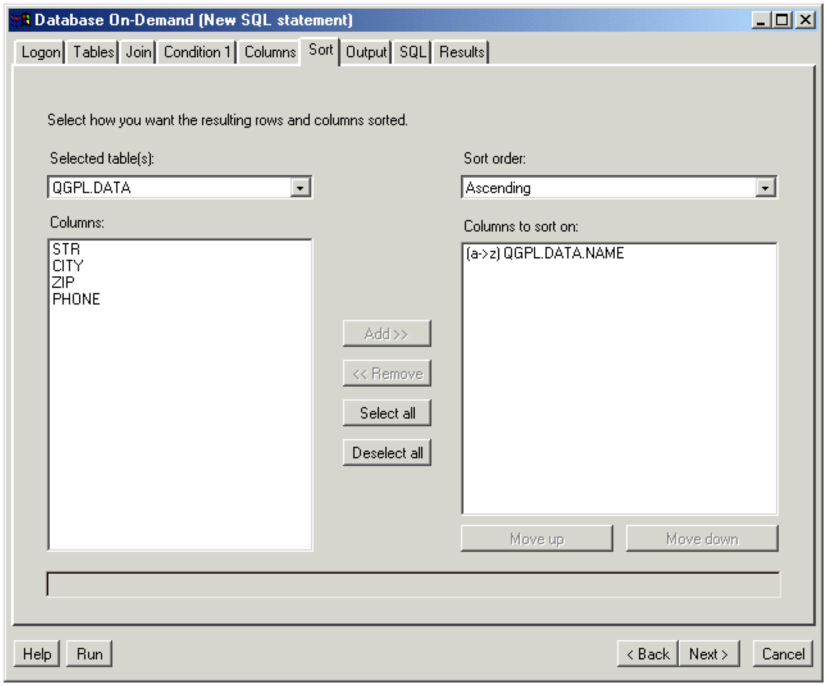
Figure 6-10 Database On-Demand column selection

Selecting a sort sequence

The Sort tab, shown in Figure 6-11, allows you to specify the sort order for the columns you included in column selection. You can sort in either ascending (a->z) or descending (z->a) order. We will sort on ascending on the Name column, so the procedure is as follows:

1. In the left-hand pane labeled Column, click **NAME**.
2. Confirm the sort order is Ascending, which is the default.
3. Click **Add >>**.
4. Click **Next** or **Output** to continue.

If you are sorting on more than one column, you have the ability to change the order in which the columns are sorted by moving them up or down in the right-hand pane labeled Columns to sort on.



Select how you want the resulting rows and columns sorted.

Selected table(s): QGPL.DATA

Sort order: Ascending

Columns:

STR
CITY
ZIP
PHONE

Columns to sort on:

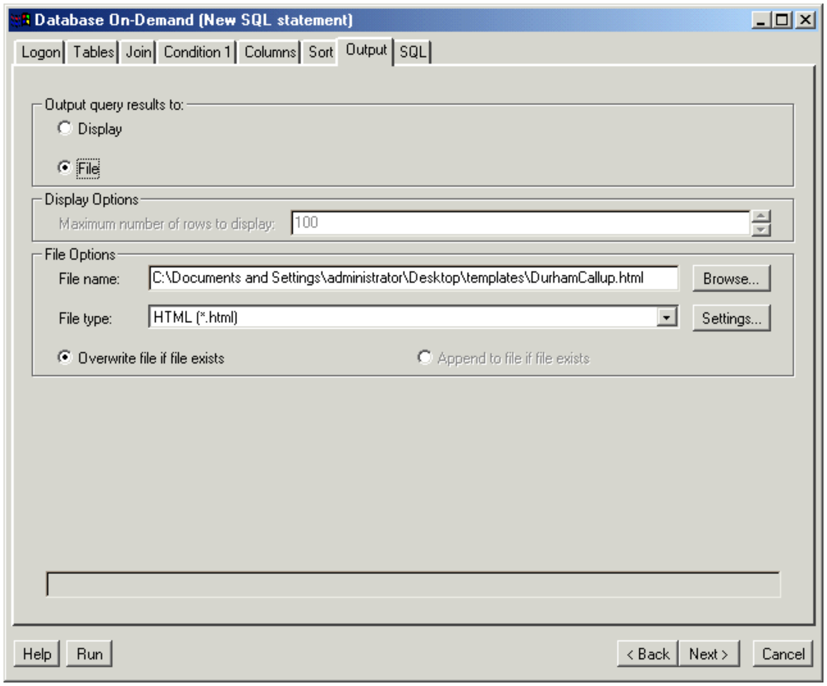
(a->z) QGPL.DATA.NAME

Figure 6-11 Database On-Demand Sort tab

Selecting the output target

The Output window, as shown in Figure 6-12, lets you send the query results to the display or to a file. Sending it to the display is quite simple, and generally the defaults provided on this window will be suitable. When sending the output to a file, there are various file types available, and in this case, we will send it to an HTML file. We will also use another HTML as a template for the results.

1. Under Output query results to, click **File**.



Output query results to:

○ Display

● File

Display Options

Maximum number of rows to display: 100

File Options

File name: C:\Documents and Settings\administrator\Desktop\templates\DurhamCallup.html

File type: HTML (*.html)

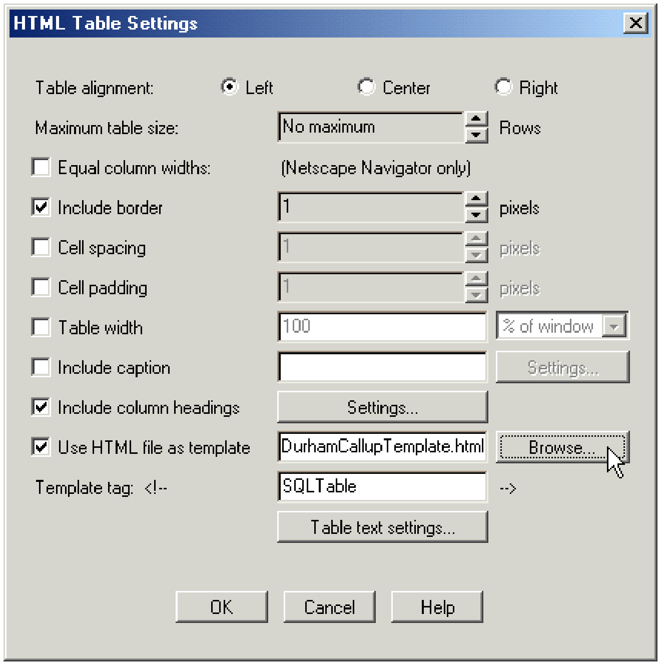
● Overwrite file if file exists ○ Append to file if file exists

Figure 6-12 Selecting the output destination

2. Type in the file name.
3. Select **HTML** as the file type.
4. Click **Settings**.

   You will be presented with the HTML Table Settings window (Figure 6-13).
5. Click **Use HTML File as template**, and either type in the file name, or locate the file using the **Browse** button.

   In this example, we will use DurhamCallupTemplate.html, the contents of which can be seen in Example 6-1 on page 253. This HTML file was created earlier using an editor such as NotePad. When using an HTML template, the default is to have the HTML comment line SQLTable replaced with the query results. This can also be modified by changing the Template Tag field.



HTML Table Settings

Table alignment: ● Left ○ Center ○ Right

Maximum table size: No maximum Rows

□ Equal column widths: (Netscape Navigator only)

☑ Include border 1 pixels

□ Cell spacing 1 pixels

□ Cell padding 1 pixels

□ Table width 100 % of window

□ Include caption

☑ Include column headings

☑ Use HTML file as template DurhamCallupTemplate.html

Template tag: <!-- SQLTable -->

Figure 6-13 HTML table settings, specifying an HTML template file

6. Click **OK** to close the HTML Table Settings window.
7. Click **Next** or the **SQL** tab to continue.

Example 6-1 Contents of DurhamCallupTemplate.html

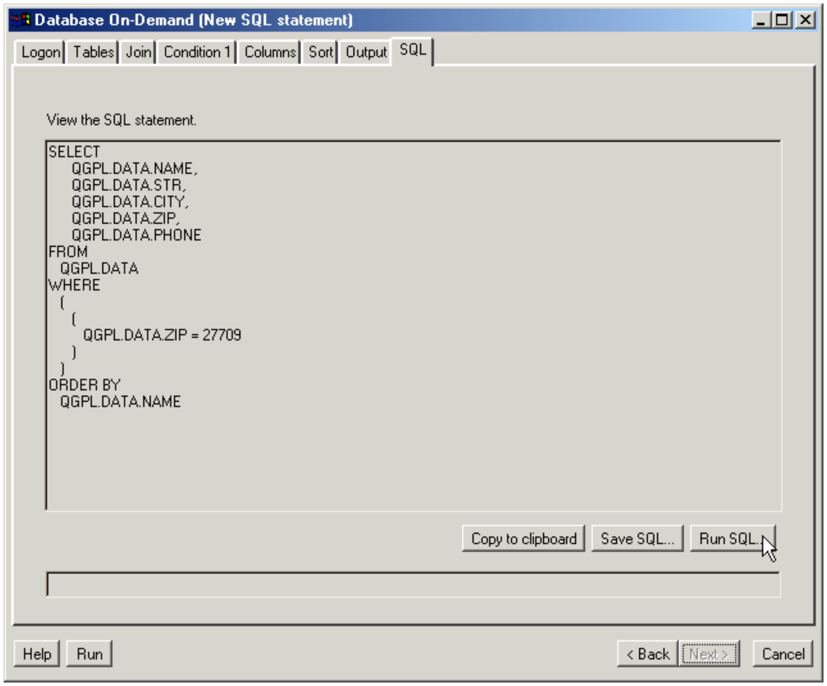
```
<HTML>
<HEAD>
<META content="text/html">
<title>Durham Callup Listing</title>
</HEAD>
<BODY>
<img src="hodlogo.gif">
<h3>Durham (27709) Callup Listing</h3>

<!-- SQLTable -->

<font size ="-1">This is a listing for all people with a 27709 zipcode</font>
</BODY>
</HTML>
```

Viewing, saving, and running the SQL

The SQL window will appear as shown in Figure 6-14 as the default. If the administrator has checked **Allow manual editing of SQL statements** when configuring your user ID or group, it appears as the window shown in Figure 6-15. Either window presented allows the user to copy the SQL to the clipboard, save the SQL, or run the query.

Executing the query can be done one of two ways:

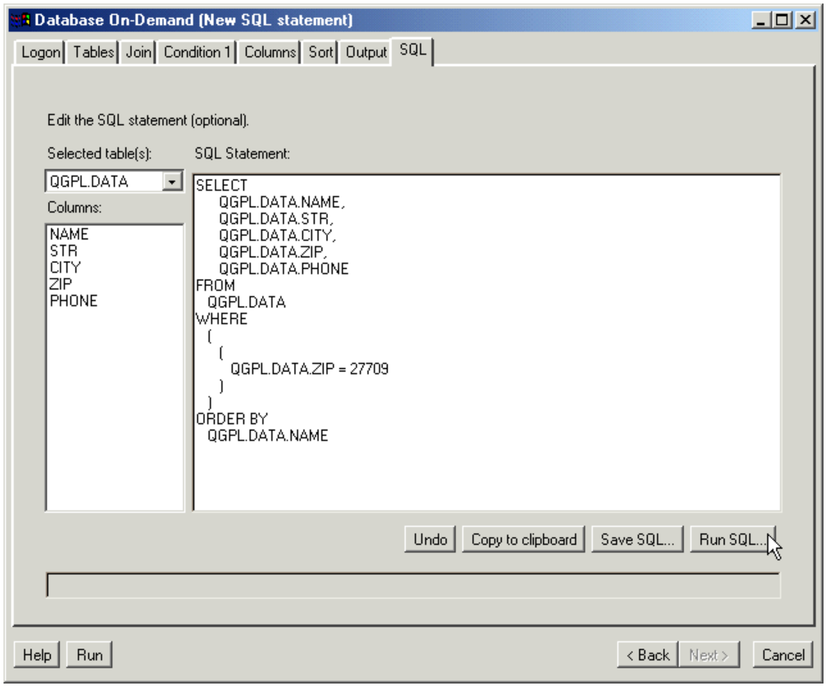
- Click **Run SQL**.
- Click the **Run** button in the bottom left-hand corner of the window.



View the SQL statement.

```
SELECT
    QGPL.DATA.NAME,
    QGPL.DATA.STR,
    QGPL.DATA.CITY,
    QGPL.DATA.ZIP,
    QGPL.DATA.PHONE
FROM
  QGPL.DATA
WHERE
  (
    (
      QGPL.DATA.ZIP = 27709
    )
  )
ORDER BY
  QGPL.DATA.NAME
```

Figure 6-14 SQL tab as the default, with no SQL editing enabled



Edit the SQL statement (optional).

Selected table(s): QGPL.DATA

Columns:

```
NAME
STR
CITY
ZIP
PHONE
```

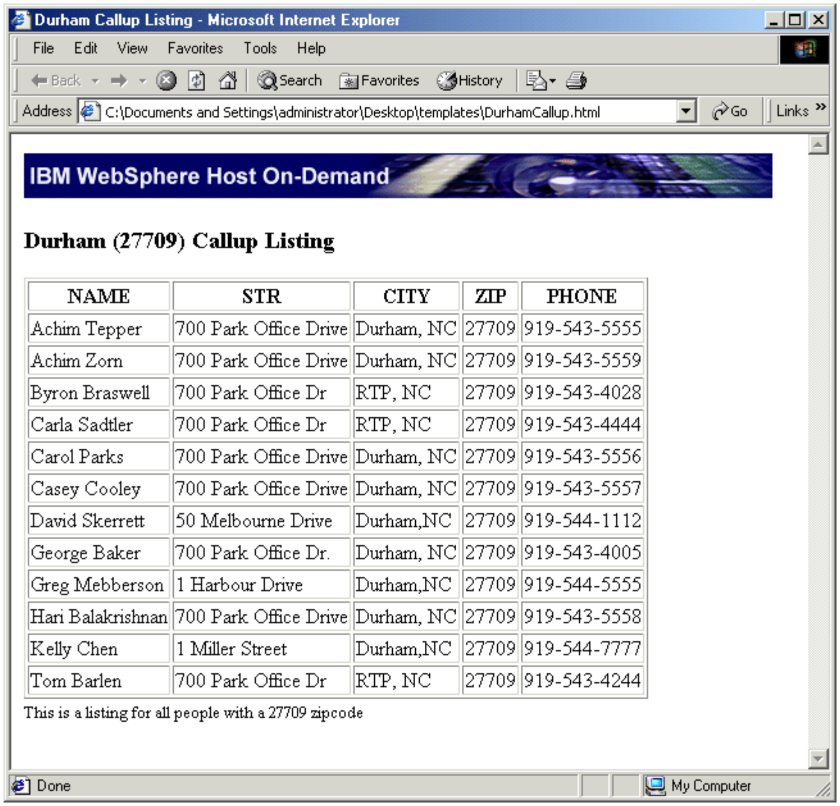
SQL Statement:

```
SELECT
    QGPL.DATA.NAME,
    QGPL.DATA.STR,
    QGPL.DATA.CITY,
    QGPL.DATA.ZIP,
    QGPL.DATA.PHONE
FROM
  QGPL.DATA
WHERE
  (
    (
      QGPL.DATA.ZIP = 27709
    )
  )
ORDER BY
  QGPL.DATA.NAME
```

Figure 6-15   SQL tab showing manual editing of SQL enabled

Viewing the results

In this example, the results were written to an HTML file, and the output can be seen in Figure 6-16.


Durham Callup Listing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Documents and Settings\administrator\Desktop\templates\DurhamCallup.html
Go Links
IBM WebSphere Host On-Demand
Done
My Computer

Durham (27709) Callup Listing

NAME	STR	CITY	ZIP	PHONE
Achim Tepper	700 Park Office Drive	Durham, NC	27709	919-543-5555
Achim Zorn	700 Park Office Drive	Durham, NC	27709	919-543-5559
Byron Braswell	700 Park Office Dr	RTP, NC	27709	919-543-4028
Carla Sadtler	700 Park Office Dr	RTP, NC	27709	919-543-4444
Carol Parks	700 Park Office Drive	Durham, NC	27709	919-543-5556
Casey Cooley	700 Park Office Drive	Durham, NC	27709	919-543-5557
David Skerrett	50 Melbourne Drive	Durham,NC	27709	919-544-1112
George Baker	700 Park Office Dr.	Durham, NC	27709	919-543-4005
Greg Mebberson	1 Harbour Drive	Durham,NC	27709	919-544-5555
Hari Balakrishnan	700 Park Office Drive	Durham, NC	27709	919-543-5558
Kelly Chen	1 Miller Street	Durham,NC	27709	919-544-7777
Tom Barlen	700 Park Office Dr	RTP, NC	27709	919-543-4244

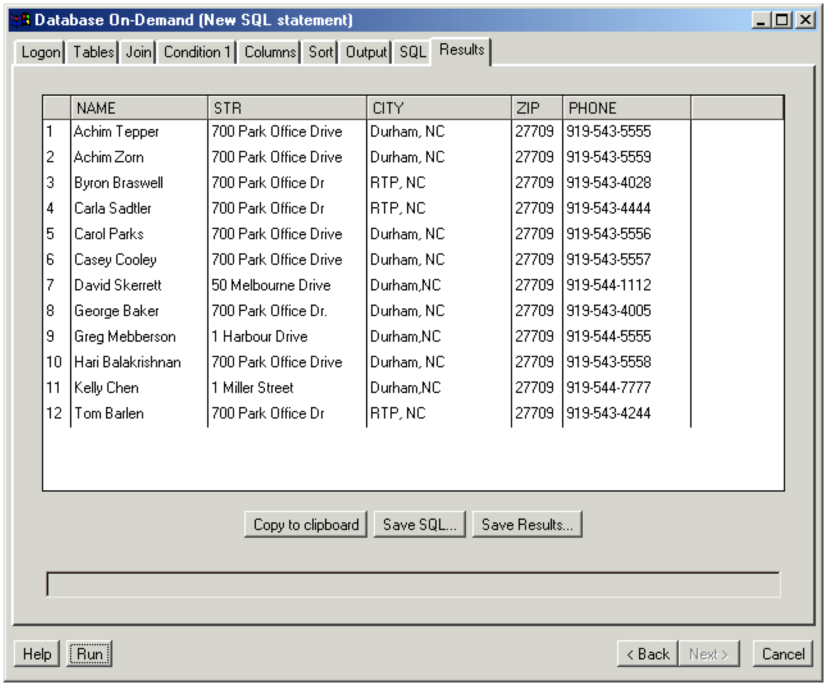
This is a listing for all people with a 27709 zipcode

Figure 6-16 Results of SQL query when viewed in a browser

If instead it is decided to send the results to the display, it will appear as shown in Figure 6-17. From this window, you can copy the results to the clipboard, save the SQL, and save the results.

If you click **Save SQL**, the statements are saved in a file called DBX.userid (where `userid` is your user ID) in the HostOnDemand\private directory on the server, with a name that you are asked to provide.

If you want to save the results of the query, click **Save Results**. The file types are the same as those provided on the Output tab, and it is possible to write it to the same HTML file using a template, as we have done earlier.



	NAME	STR	CITY	ZIP	PHONE
1	Achim Tepper	700 Park Office Drive	Durham, NC	27709	919-543-5555
2	Achim Zorn	700 Park Office Drive	Durham, NC	27709	919-543-5559
3	Byron Braswell	700 Park Office Dr	RTP, NC	27709	919-543-4028
4	Carla Sadtler	700 Park Office Dr	RTP, NC	27709	919-543-4444
5	Carol Parks	700 Park Office Drive	Durham, NC	27709	919-543-5556
6	Casey Cooley	700 Park Office Drive	Durham, NC	27709	919-543-5557
7	David Skerrett	50 Melbourne Drive	Durham,NC	27709	919-544-1112
8	George Baker	700 Park Office Dr.	Durham, NC	27709	919-543-4005
9	Greg Mebberson	1 Harbour Drive	Durham,NC	27709	919-544-5555
10	Hari Balakrishnan	700 Park Office Drive	Durham, NC	27709	919-543-5558
11	Kelly Chen	1 Miller Street	Durham,NC	27709	919-544-7777
12	Tom Barlen	700 Park Office Dr	RTP, NC	27709	919-543-4244

Figure 6-17 Results when sent to the display

When you have finished with this query, you can either modify the query and re-run it, save the SQL, or click **Cancel** to end the query.

6.2.2 Running an SQL statement

You can run any SQL statement that is listed on your Saved SQL Statements list.

To run a query, highlight the statement you want to use, then click **Run**. When the query has run, the results will be displayed.

If you did not select **Save password with statement** when saving the SQL, you will be prompted for your password prior to the SQL running.

6.2.3 Changing an SQL statement

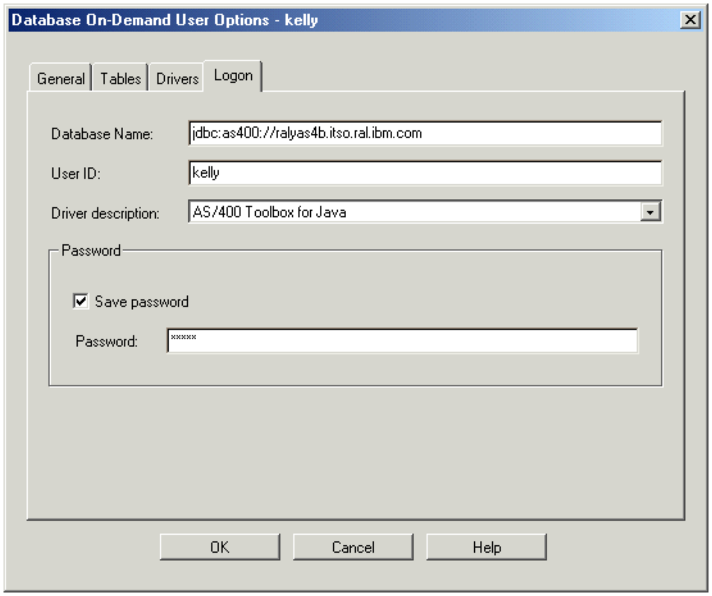
You can view and edit the options used to create an existing SQL statement. This lets you make changes without having to recreate the SQL each time.

6.2.4 Deleting an SQL statement

You can delete SQL statements from your SQL Statements window, but once they are deleted, they cannot be recovered. SQL statements saved at the group level must be removed by the administrator. Icons alongside the SQL statement indicate whether it is at the group or individual level.

6.2.5 Customizing user options

Users can customize the behavior of Database On-Demand to suit their needs. For example, if you are always connecting to the same server, you can save the default logon values for the database name, user ID, password, and driver to be used, as shown in Figure 6-18.



Database Name: jdbc:as400://ralyas4b.itso.ral.ibm.com

User ID: kelly

Driver description: AS/400 Toolbox for Java

Password

☑ Save password

Password: *****

Figure 6-18 Setting default logon parameters

6.3 Installing and registering other JDBC drivers

There are now many JDBC drivers available, although only the iSeries driver is provided and supported with Database On-Demand.

By way of example, let us install the JDBC driver for IBM DB2 so that you can use Database On-Demand to access DB2 databases. The DB2 JDBC driver is in the db2java.zip file, which is located in [drive::]\SQLLIB\java\ after the installation of the CAECLIENT.

6.3.1 Installing a driver

New JDBC drivers must be installed in the same directory path as the AS/400 driver that is provided with Host On-Demand. For example, if the current directory for the default AS/400 JDBC driver is:

```
[drive:]\hostondemand\HOD\com\ibm\as400\access
```

Where `drive` is the drive letter where Host On-Demand is installed, you must unpack db2java.zip to `[drive:]\hostondemand\HOD` and the following directory structure will be created for the applet driver:

```
[drive:]\hostondemand\HOD\com\ibm\db2\jdbc\net\DB2Driver
```

6.3.2 Registering a driver

Either an administrator or user can register a driver. The procedures are as follows.

Registration by the administrator

Administrative registration begins by opening the Database On-Demand Options window by right-clicking either a group or user and selecting **Database > Options...** as shown in Figure 6-1 on page 241.

1. Click the **Driver** tab (see Figure 6-19).
2. Type in a description for the driver; in this example we entered:

   ```
   DB2 Applet driver
   ```
3. Type in the class name of the driver, *ensuring the case is correct*:

   ```
   COM.ibm.db2.jdbc.net.DB2Driver
   ```

   The class extension is not specified.
4. Click **Register Driver**.
5. Click **OK** to save the new drivers.

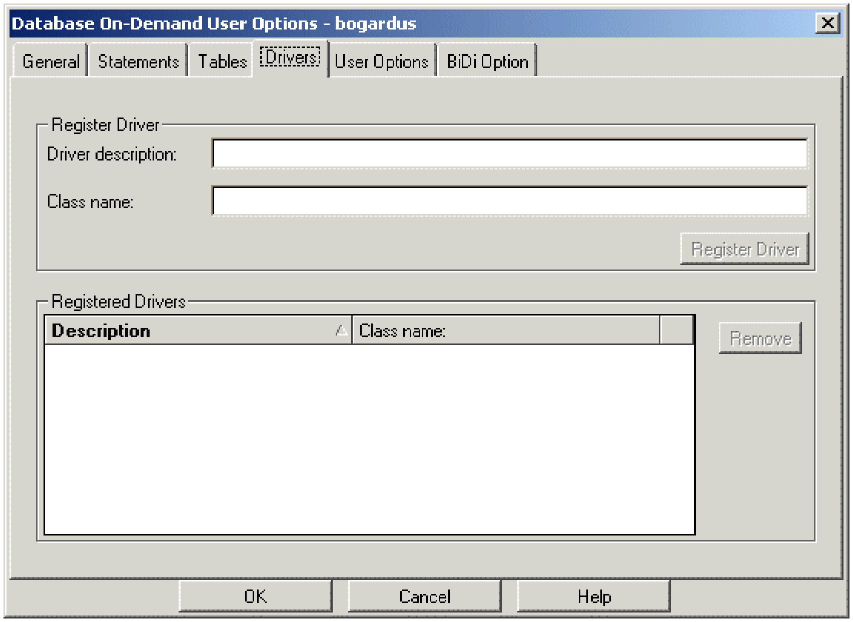


Figure 6-19 Registering DB2 JDBC driver by the administrator

Registration by a user

To register a driver, you must click **Options** on the initial Database On-Demand window. From this point you should follow the numbered steps in “Registration by the administrator” on page 259.

6.3.3 Using a new driver

Start a new SQL query from the Database On-Demand applet (see Figure 6-6 on page 245):

1. Click **New**.

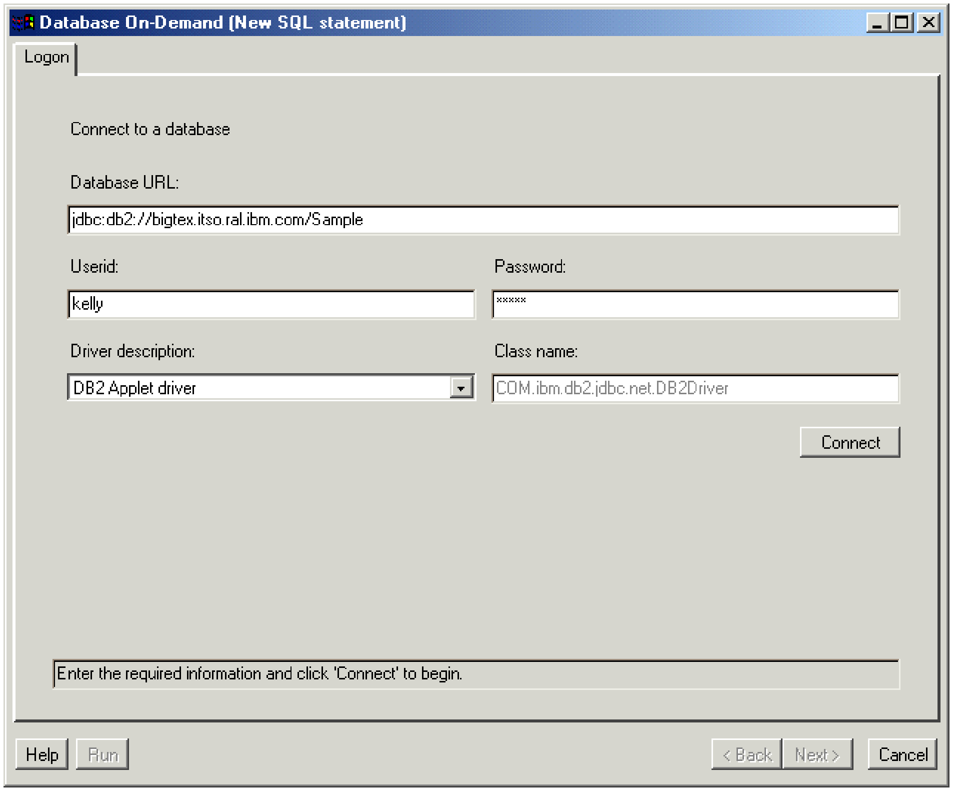
   You will then see the Logon tab similar to Figure 6-20. This window is shown with all steps completed, and ready to connect to a DB2 database.

2. Type in the Database URL, such as:

   ```
   jdbc:db2://bigtex.itso.ral.ibm.com/Sample
   ```

3. Fill in the Userid and Password fields.
4. In the Driver description, from the drop-down list select the DB2 driver that you just registered, DB2 Applet driver. You will see the Class name change to the correct driver.
5. Click **Connect**.

Once connected, generating an SQL statement and navigating the windows is the same as for the iSeries database, explained earlier in 6.2.1, “Creating a new SQL statement” on page 246.



Connect to a database

Database URL: jdbc:db2://bigtex.itso.ral.ibm.com/Sample

Userid: kelly

Password: *****

Driver description: DB2 Applet driver

Class name: COM.ibm.db2.jdbc.net.DB2Driver

Enter the required information and click 'Connect' to begin.

Figure 6-20 Connecting to a DB2 database

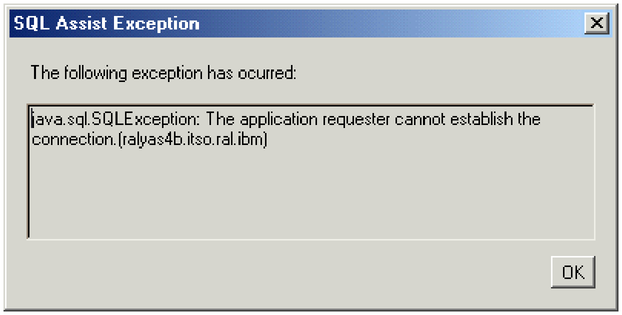
> **Note:** The DB2 database must reside on the Web server, otherwise, a Security Exception will occur. The JDBC driver will attempt to establish a separate network connection with the DB2 database through the JDBC applet server residing on the Web server. Java will trigger a security exception if the servers are different. More information can be found in the online *DB2 Application Building Guide*.

6.3.4 Common access problems

Sometimes, when you try to connect to a database, an SQL Assist Exception occurs. Such exceptions generally indicate that something on the Logon window is incorrect. In the following are some examples of exceptions that can occur.

Application requester cannot establish the connection

Check that you entered the database name completely. For example, the error shown in Figure 6-21 can occur if the name is as400.raleigh.ibm.com®, but you only typed `as400` and this host name cannot be resolved by a name server.



The following exception has ocurred:

java.sql.SQLException: The application requester cannot establish the connection.(ralyas4b.itso.ral.ibm)

Figure 6-21 Error establishing database connection

No suitable driver

The no suitable driver error, shown in Figure 6-22, can occur if any part of the database name is incorrect. Below are some common errors:

- Correct syntax:

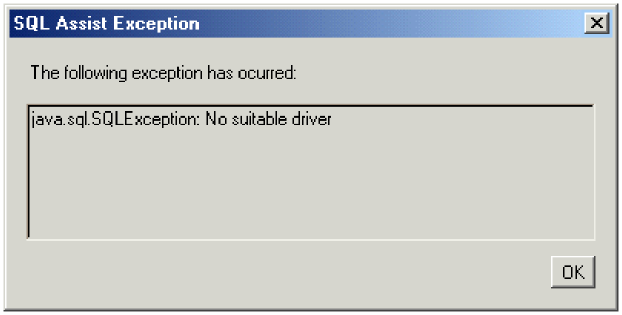
  ```
  jdbc:as400://bigtex.raleigh.ibm.com
  ```

- Incorrect syntax:

  ```
  jdbc:as400//bigtex.raleigh.ibm.com
  ```

- Incorrect syntax:

  ```
  jdbc:as40://bigtex.raleigh.ibm.com
  ```



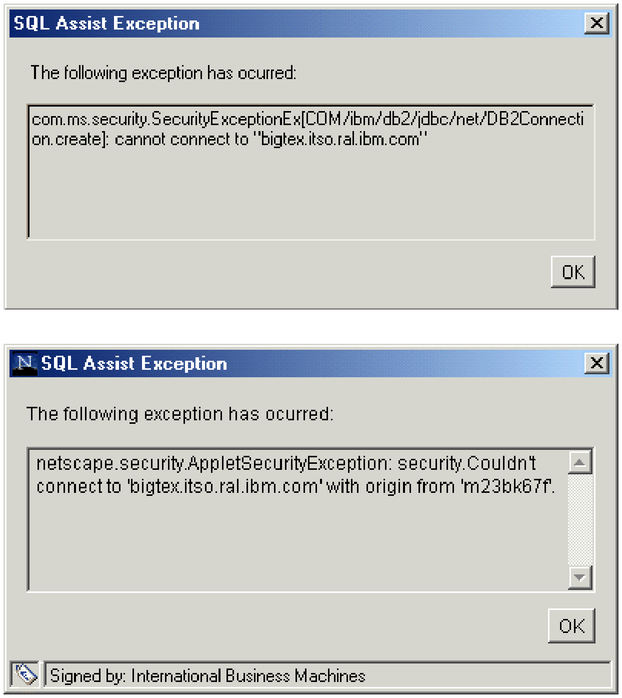
The following exception has ocurred:

java.sql.SQLException: No suitable driver

Figure 6-22 Error finding driver

Security exception

If you attempt to access a DB2 database that resides on a server different from the one that served the applet, you will receive a security exception as shown in Figure 6-23. This type of activity violates Java security. In our example, the DB2 database is on bigtex.itso.ral.ibm.com, and the Web server is on mk23bk67f. Internet Explorer and Netscape Navigator report the error differently. The error window shown at the top of Figure 6-23 is generated by Microsoft Internet Explorer, while the error window generated by Netscape Navigator is shown at the bottom.



The following exception has ocurred:

```
com.ms.security.SecurityExceptionEx[COM/ibm/db2/jdbc/net/DB2Connecti
on.create]: cannot connect to "bigtex.itso.ral.ibm.com"
```

The following exception has ocurred:

```
netscape.security.AppletSecurityException: security.Couldn't
connect to 'bigtex.itso.ral.ibm.com' with origin from 'm23bk67f'.
```

Signed by: International Business Machines

Figure 6-23 Error when attempting to connect to a remote DB2 database

7

Administration

The Service Manager is the component of Host On-Demand that controls the following Host On-Demand functions and the data stored on the Host On-Demand server:

- Users/group management (configuration server)
- Services management
- Redirector Service management
- Directory Service management
- OS/400 Proxy Server management
- License use management

Administration of a Host On-Demand server is done primarily through the administration applet, HODAdmin.html, which is loaded into your browser. If you are working on a Windows NT, Windows 2000, or Windows XP, click **Start -> Programs -> IBM Host On-Demand -> Administration -> Administration Utility**. On all other platforms or at a workstation, load the applet by entering the following URL:

```
http://[server_name]/hod/HODAdmin.html
```

For access to the administrative functions, you must log on using an administrative user ID and password. The default user ID supplied by Host On-Demand is `admin` and the default password is `password`.

7.1 Managing users and groups

The Users/Groups task of the Administration Notebook, shown in Figure 7-1, lets you:

- Manage groups

  If you are using an LDAP directory to store configuration information (see 7.4, “Directory service” on page 348), groups may be hierarchical. The default data store does not allow for hierarchical groups.

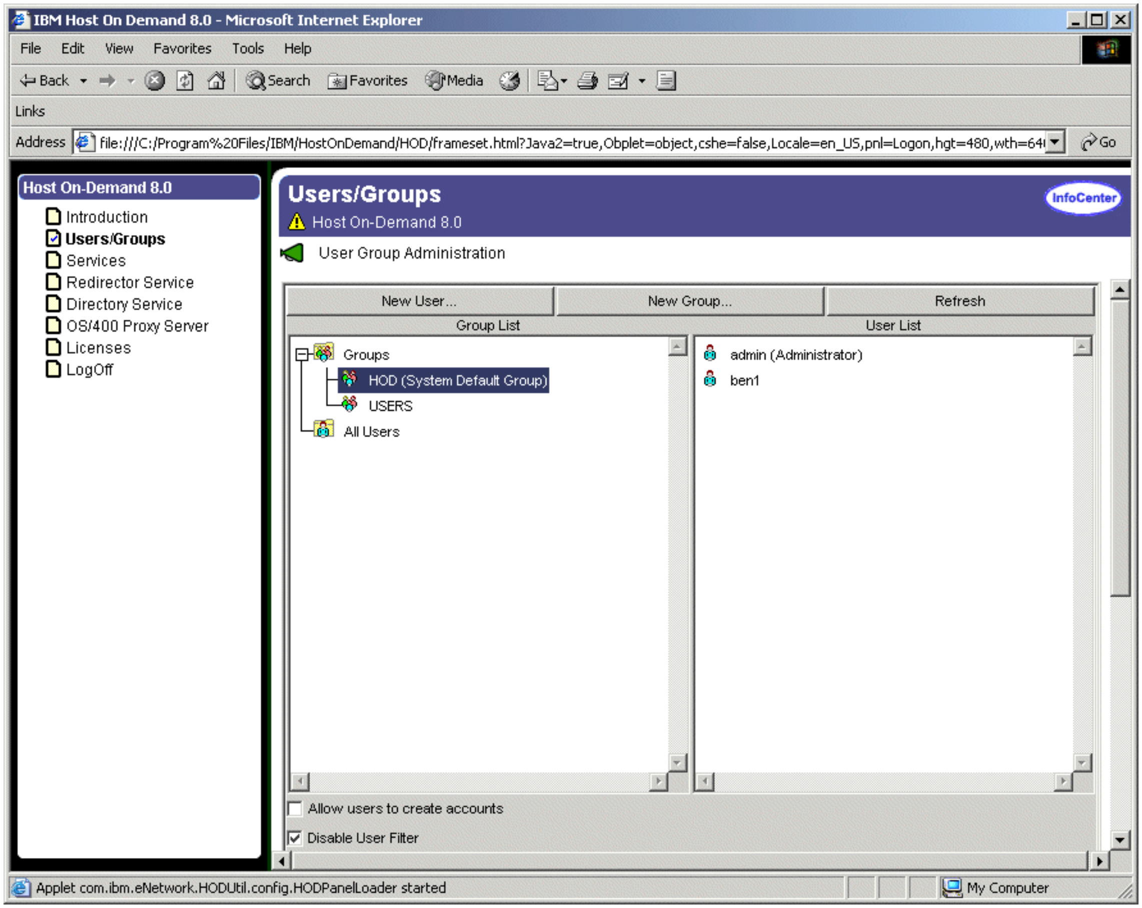
- Manage users

  If you are using the default data store, users may belong to multiple groups; however, if you are using an LDAP directory to store preferences (see 7.4, “Directory service” on page 348), a user may belong to only one group.

- Manage sessions for users or groups

  If you create a session for a group, all the users that you assign to that group inherit the session and all its settings.

- Copy, change, and delete users, groups, and sessions.
- Look at a trace file that has been created by a user and saved to the server.



Address: file:///C:/Program%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=64

□ Allow users to create accounts

☑ Disable User Filter

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 7-1 Users/Groups Administration window

When dealing with a large number of groups, users, or sessions, you may find it convenient to use Directory Utility. Directory Utility is a command-line Java application the administrator can use to manage user, group, and session configuration information. Directory Utility reads an XML ASCII file that contains the following actions to be performed on users, groups, and sessions defined to the configuration server:

- Add, update, and delete groups
- Add, update, and delete users from groups
- Add, update, and delete sessions from users or groups

For details, see 7.7, "Directory Utility" on page 358.

7.1.1 Planning

Host On-Demand Version 8 offers three different deployment models:

1. Configuration Server model

   Initial configuration data is stored at the server, and user modifications are stored on the server.

2. The HTML-based model

   The configuration is deployed in a customized HTML file, and user modifications are saved locally at the client system.

3. The combined model

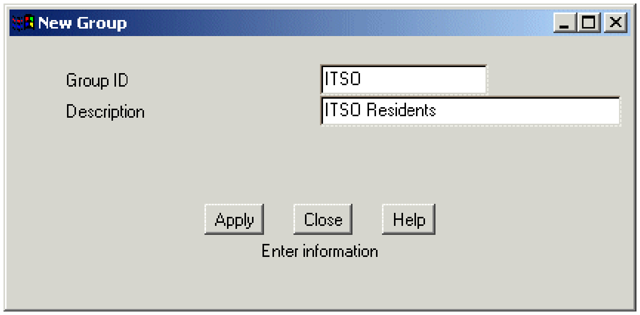
   The client retrieves the group configuration from the server; however, user modifications are saved locally at the client system.

See Chapter 13, “Deployment strategies” on page 501 for a detailed explanation of these models.

7.1.2 Managing groups

Each user must be a member of at least one group. You may use the Host On-Demand provided default group, HOD, or you may create a group into which you will add users. When using the default data store, all groups are at the same level, and users may belong to multiple groups. However, if you store your preferences in an LDAP directory, you may organize your groups hierarchically, but a user belongs to a single group and its hierarchy.

To add a new group, click **New Group.** If you are using the default data store, the window shown in Figure 7-2 will appear; and if you are using an LDAP directory, the window shown in Figure 7-3 will appear.


New Group

Group ID: ITSO

Description: ITSO Residents

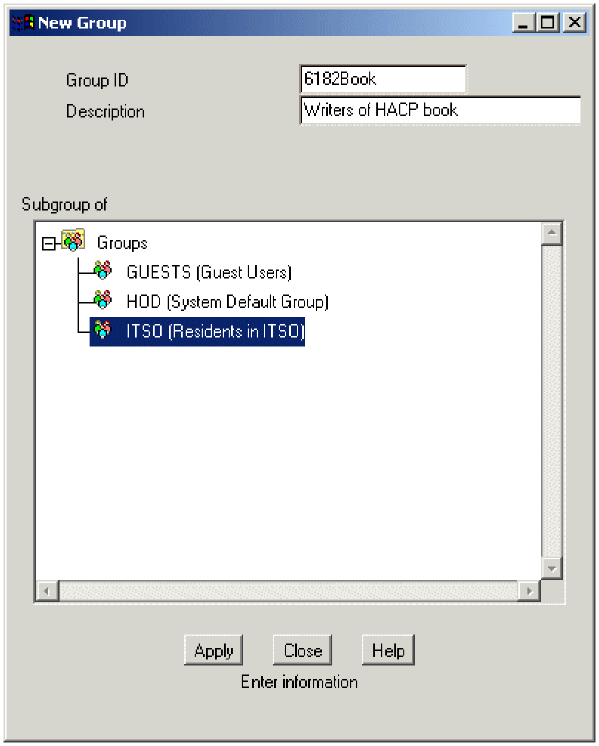
Enter information

Figure 7-2 Configuring a group with default data store

You must enter a group ID. The first character must be a letter, and all other characters must be the English equivalent of A-Z, a-z, 0-9, . (period), and - (hyphen). Group IDs are always converted to uppercase unless you are using an LDAP directory server data store where mixed-cased characters are allowed.

A group description is optional. Any character is allowed except | (vertical bar) or # (number or pound sign).

If you are using the LDAP directory, you must select the hierarchy that the group will occupy. In the example shown in Figure 7-3, the group 6182book will be added under the group ITSO. The net result is that any user in the 6182book group will inherit sessions defined at the ITSO and the 6182books group level.



Group ID: 6182Book

Description: Writers of HACP book

Subgroup of

- Groups
  - GUESTS (Guest Users)
  - HOD (System Default Group)
  - ITSO (Residents in ITSO)

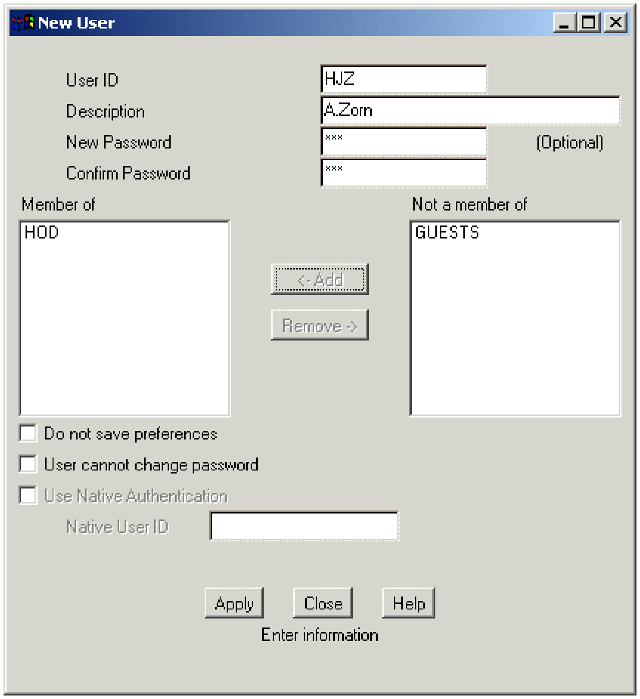
Enter information

Figure 7-3 New group with LDAP

To store the group, click **Apply.** The window will remain open so that you may add another group. When you are finished adding groups, click **Close**.

7.1.3 Creating a new user

To add a new user, click **New User**. If you are not using the LDAP directory to store preferences, the window shown in Figure 7-4 will appear.



New User

User ID: HJZ

Description: A.Zorn

New Password: *** (Optional)

Confirm Password: ***

Member of: HOD

Not a member of: GUESTS

☐ Do not save preferences

☐ User cannot change password

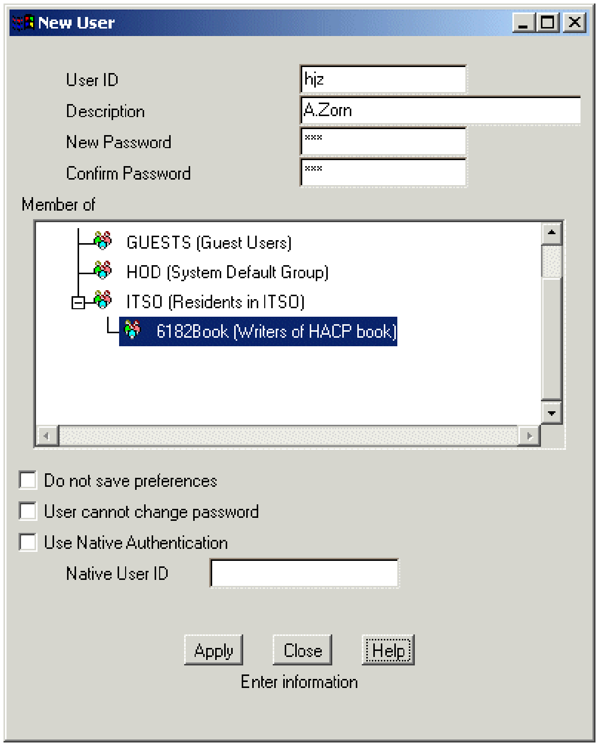
☐ Use Native Authentication

Native User ID

Enter information

Figure 7-4 Configuring a user with local data store

If you are using the LDAP directory server for preferences, you will see the window shown in Figure 7-5.



New User

User ID hjz

Description A.Zorn

New Password ***

Confirm Password ***

Member of

GUESTS (Guest Users)

HOD (System Default Group)

ITSO (Residents in ITSO)

6182Book (Writers of HACP book)

□ Do not save preferences

□ User cannot change password

□ Use Native Authentication

Native User ID

Enter information

Figure 7-5 New user with LDAP directory

You must now complete the following elements of the window:

- User ID

  The Host On-Demand user ID being created. The first character must be a letter. Valid characters are A-Z, a-z, 0-9, . (period), and - (hyphen). When using Host On-Demand to store configuration information, user IDs are converted to lowercase characters. User IDs must be unique, and must not match group IDs regardless of case.

  > **Note:** Windows users can define Host On-Demand user IDs that are identical to their corresponding Windows domain user IDs, users who log on to their Windows domain user IDs do not have to log in again to access their Host On-Demand sessions.

- Description (optional)

A brief description of the user ID being created. Suggested contents: the full name of the user or a description of a group for a shared user ID. You can use any character except | (vertical bar) and # (number or pound sign).

- New Password (optional)

  The user's password. Passwords are not required.

- Confirm Password (optional)

  Repeat User's Password for confirmation. Not available when **Native Authentication** is selected.

- Member of

  Each user must be a member of at least one group. If you are using LDAP, a user can be a member of only one group. Select the group of which you want the user to be a member. Unlike default Host On-Demand users, natively authenticated users cannot belong to multiple groups. The first character must be a letter. Valid characters are A-Z, a-z, 0-9, . (period), and - (hyphen). Group IDs are always converted to uppercase if the default Host On-Demand data store is used.

  Note: When using the default data store, we recommend that you not place more than 1000 users in any one group.

- Do not save preferences

  If selected, the user may be able to change items, such as emulator colors, but the changes will not be saved.

  Users can be denied access to making preference changes. See 6.1.8, "Disabling emulator functions" on page 211 for details.

- User cannot change password

  Prohibits a user from changing their password. When defining a natively authenticated user, this will be selected automatically.

- Use Native Authentication

  Select this box to use the Native Authentication feature (only enabled when LDAP is used). Refer to 7.1.4, "Using Native Authentication" on page 273.

- Native User ID

  This is the user ID that will be passed to the native operating system. This can be different from the Host On-Demand user ID. See 7.1.4, "Using Native Authentication" on page 273. If you are running on an AIX or UNIX operating system, ensure that this ID is set to the proper case, because IDs are case sensitive in these environments.

7.1.4 Using Native Authentication

The native platform authentication service allows users to log on to Host On-Demand using the same password that they would use to log on to the operating system (Windows NT, AIX or z/OS) where Host On-Demand is active. When a user logs on to Host On-Demand, their password is validated against the system password, rather than a separate Host On-Demand password. This gives the administrator a single point of control for password administration, and the user a single password to remember.

When a user logs on, the following sequence (as shown in Figure 7-6) takes place:

1. The user ID and password are sent to the Host On-Demand service manager.
2. The service manager sends a request for logon information about the user to the LDAP server.
3. The LDAP server returns the requested user information and whether or not the user is configured for native authentication.
4. If the user is configured to use native authentication, the service manager sends the authentication user ID and the password to the operating system for verification. If the user is not configured for Native Authentication, the service manager compares the password that was entered by the user with the password returned by the LDAP server.

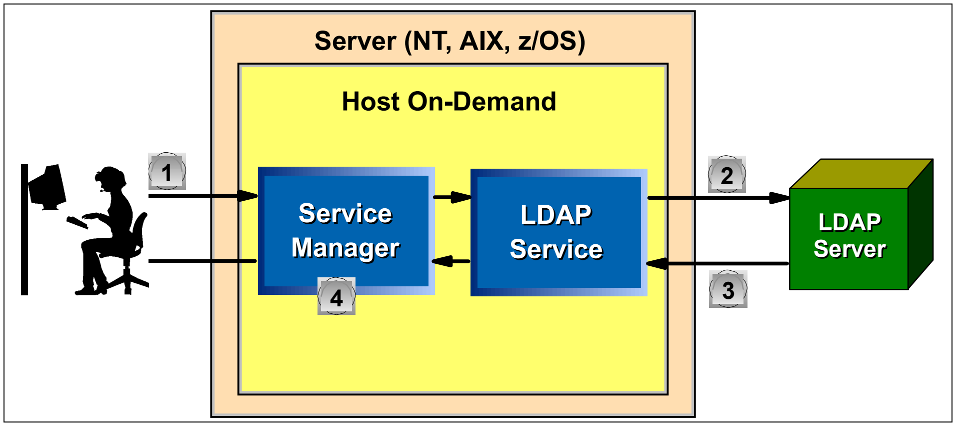
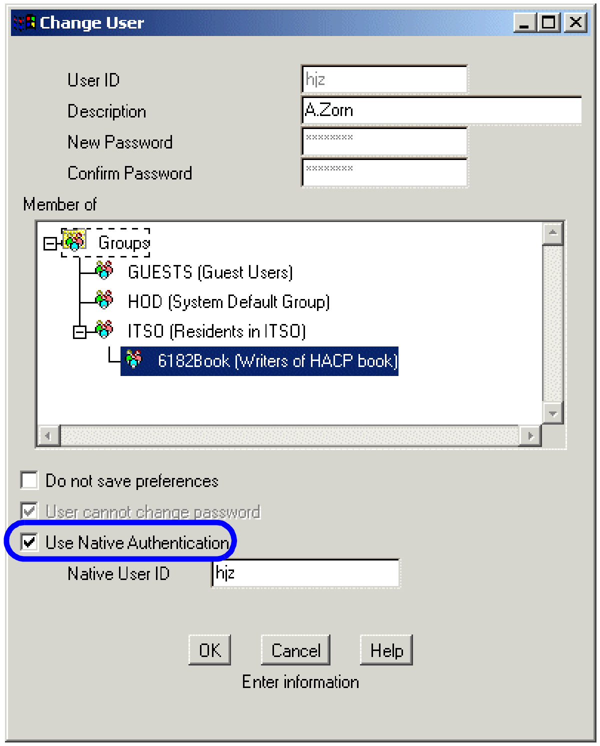


Figure 7-6 Process of Native Authentication

Use of the LDAP directory server must first be enabled as explained in 7.4, “Directory service” on page 348 in order to use Native Authentication.

To enable a user for Native Authentication, select the **Use Native Authentication** checkbox, as shown in Figure 7-7.



Change User

User ID: hjz
Description: A.Zorn
New Password: ********
Confirm Password: ********
Member of:
Groups
- GUESTS (Guest Users)
- HOD (System Default Group)
- ITSO (Residents in ITSO)
  - 6182Book (Writers of HACP book)

□ Do not save preferences
☑ User cannot change password
☑ Use Native Authentication
Native User ID: hjz

Figure 7-7 Configuring a user with Native Authentication

A bit more explanation is in order on the relationship between the Host On-Demand user ID/password and the native user ID/password. The rules are fairly simple in this relationship.

- The Host On-Demand user ID and password are a Host On-Demand administrative convenience. The user ID acts only as an index to the configuration data stored by Host On-Demand. It can be whatever you want it to be (within the Host On-Demand naming rules).
- If a password was previously specified, it will be ignored when you enable Native Authentication. It will remain in the database and if you ever disable Native Authentication for the user, it will be reactivated.
- In Native Authentication mode, all password handling is done by the native operating system; therefore, the **User cannot change password** checkbox is disabled (grayed out, see Figure 7-7). If the native password expires and the user attempts to log on to Host On-Demand, the Host On-Demand logon

will fail. The user must use an operating system interface to change the password before logging on to Host On-Demand.

- You must be careful with the native user ID if the Host On-Demand server is running on an AIX or UNIX system. On AIX and UNIX systems, the native user ID is case sensitive. Therefore, make sure the native user ID is specified with the proper case. There is no translation of this field by Host On-Demand and case sensitivity is maintained.
- By default, Host On-Demand will translate all passwords entered at the logon window to lowercase before validating them, or forwarding them to the native system for authentication. Windows, AIX and UNIX servers all respect case sensitivity when dealing with passwords; therefore, if your Host On-Demand server is running on Windows NT, AIX or any UNIX server, you should insert the following parameter into the NSMprop file (found in the /HostOnDemand/lib subdirectory) to ensure proper processing of passwords:

  ```
  LowerCasePasswords=false
  ```

  Once you set this parameter, all passwords will be case sensitive, even for those users not using Native Authentication.

7.1.5 Administering groups, sessions, and users

There is much that can be done by using standard GUI manipulation of the objects presented on the Users/Groups window shown in Figure 7-1 on page 267. All operations on Host On-Demand groups and users are performed by using the context (pop-up) menus. Operations using the context menus can be performed on only one group at a time. However, more than one user can be selected for a given operation using the mouse or the arrow key on the keyboard. Follow the standard Windows conventions. For users not familiar with Windows, the following tips will help:

- Clicking the user (or using the spacebar) with the mouse selects that user and deselects any other user(s).
- Clicking the user (or using the spacebar) while pressing the Ctrl key selects additional users.
- Clicking the user (or using the spacebar) while pressing the Shift key will select all users between one that is already selected up to and including the current user.

> **Note:** The context menu is displayed when clicking the right mouse button. It will allow only those functions that are allowed in that context. For example, defining the host sessions available to a user can be done only at the individual user, or at a single group level.

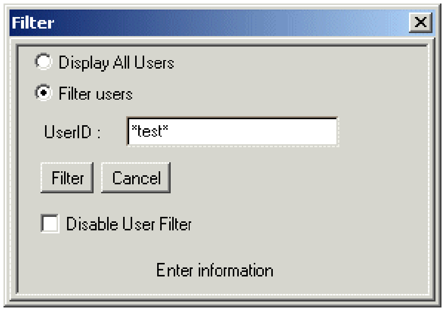
If you select the **Allow users to create accounts** checkbox in the Users/Groups window (at the bottom of Figure 7-1 on page 267), you must provide an HTML file through which the users can create their own accounts. A sample file, NewUser.html, is located in the publish directory (the default is /HostOnDemand/HOD). You can use the sample file or create customized versions of it using the Deployment Wizard. Additional information can be found in 5.5.1, “New user client” on page 165.

Note: For performance reasons, it is recommended that you place no more than 1000 users in any one group.

7.1.6 Filtering

If you have a large number of users, you may wish to use the Filter option to restrict the number of users displayed at one time. Filters are used to view the users within a group or the users in the All Users folder. There are two ways a filter can be used:

- By using the filter option of the context menu for a group. This is a one-time use of filtering that allows the administrator to view a subset of a group. If another group is selected, the administrator will be shown an unfiltered view of that group, unless the filter context menu is used for that group also.



UserID : *test*

☐ Disable User Filter

Figure 7-8 Selecting only the users containing “test” in their userids

- Globally enabling the filter option. This is set by deselecting the **Disable User Filter** checkbox in the lower left-hand corner of the User/Groups administrative window. When this is done, every time the administrator views a different group, he will be asked for a new filter to use.

If you are using the same filter to view all groups, it is advisable to copy the filter into the system clipboard and paste it into the filter window.

Note: Host On-Demand stores all user IDs in lowercase and the filter engine is case sensitive. Therefore, you should not use uppercase letters in the filter. For example, a filter on G* will not return the same list as g*.

7.1.7 Configuring sessions

If several users need the same connection, you should put them in a group and define the sessions for that group rather than defining the sessions for each user. If there are users that have unique session requirements, the sessions must be defined separately for each such user.

There is no difference if you are configuring a session for a user or a group. Simply double-click the user or group entry where you wish to define the session,j and the window shown in Figure 7-9 will appear. To add a new session, click the button for the type of session you want to configure.

From an full administrator (with start session capability), an existing session can be run directly from the administrator by pointing to the session icon, and right-clicking and selecting **Start Session** from the context menu. In this way, administrators can easily test the defined session. However, the administrator can start only one session at a time.

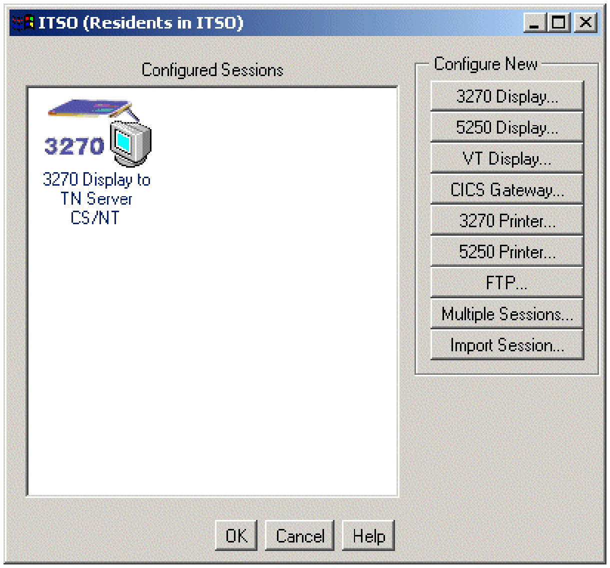
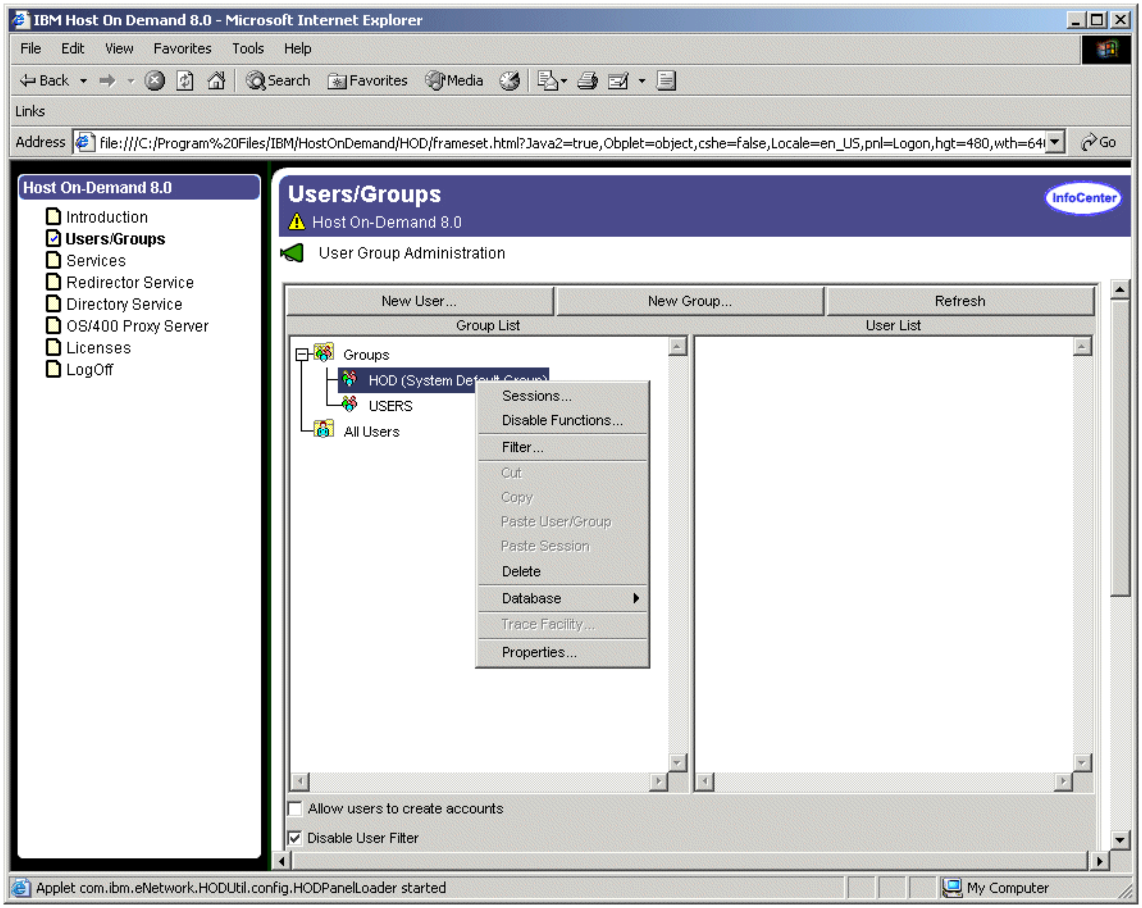


Figure 7-9 Session selection window

To copy a session display, open the context menu as shown in Figure 7-10 and click **Copy**, then find the group or user to whom you want to add the session; right-click again and click **Paste**.


IBM Host On Demand 8.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Address file:///C:/Program%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=64
Go
Host On-Demand 8.0
Introduction
Users/Groups
Services
Redirector Service
Directory Service
OS/400 Proxy Server
Licenses
LogOff
Users/Groups
Host On-Demand 8.0
InfoCenter
User Group Administration
New User...
New Group...
Refresh
Group List
User List
Groups
HOD (System Default Group)
USERS
All Users
Sessions...
Disable Functions...
Filter...
Cut
Copy
Paste User/Group
Paste Session
Delete
Database
Trace Facility...
Properties...
Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started
My Computer

☐ Allow users to create accounts

☑ Disable User Filter

Figure 7-10 Administration context menu

If you would like to copy a session within the same user or group, click the right mouse button to display the context menu and click **Duplicate Session** rather than using copy and paste.

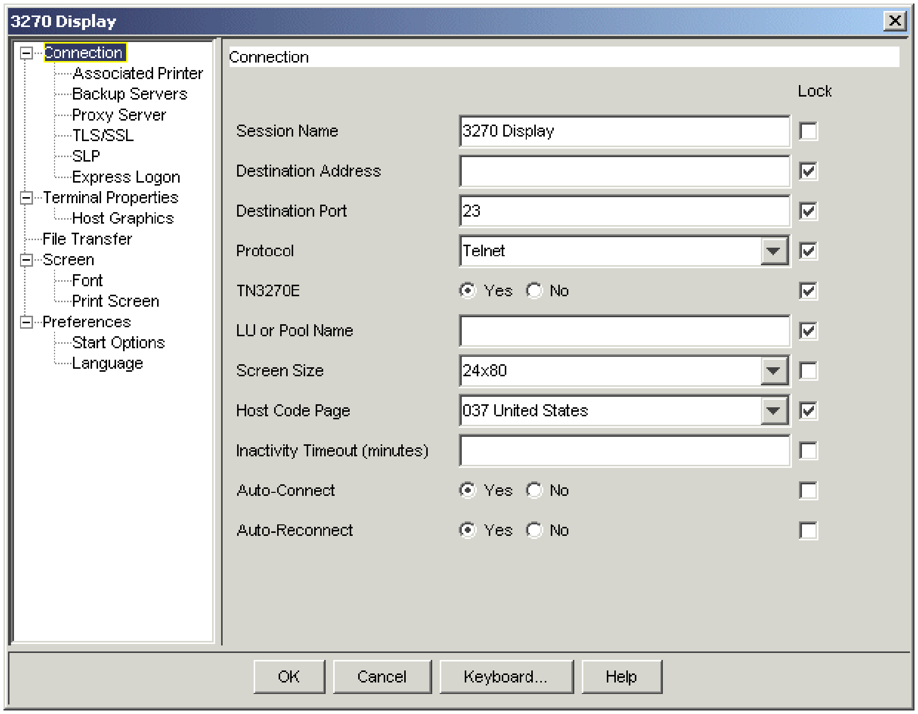
3270 and 5250 Printer Sessions

The setup of 3270 and 5250 Printer Sessions is similar to the display sessions. For parameters specific to print sessions, please refer to Chapter 21, “Printing” on page 713.

3270 and 5250 Display Sessions

The 3270 and 5250 sessions are very similar. The 3270 sessions will be used as an example except where there is a significant difference in the fields, then both will be explained. Fields unique to a specific emulator type are highlighted.

Selecting **3270 Display** from the window shown in Figure 7-9 brings up the window shown in Figure 7-11.

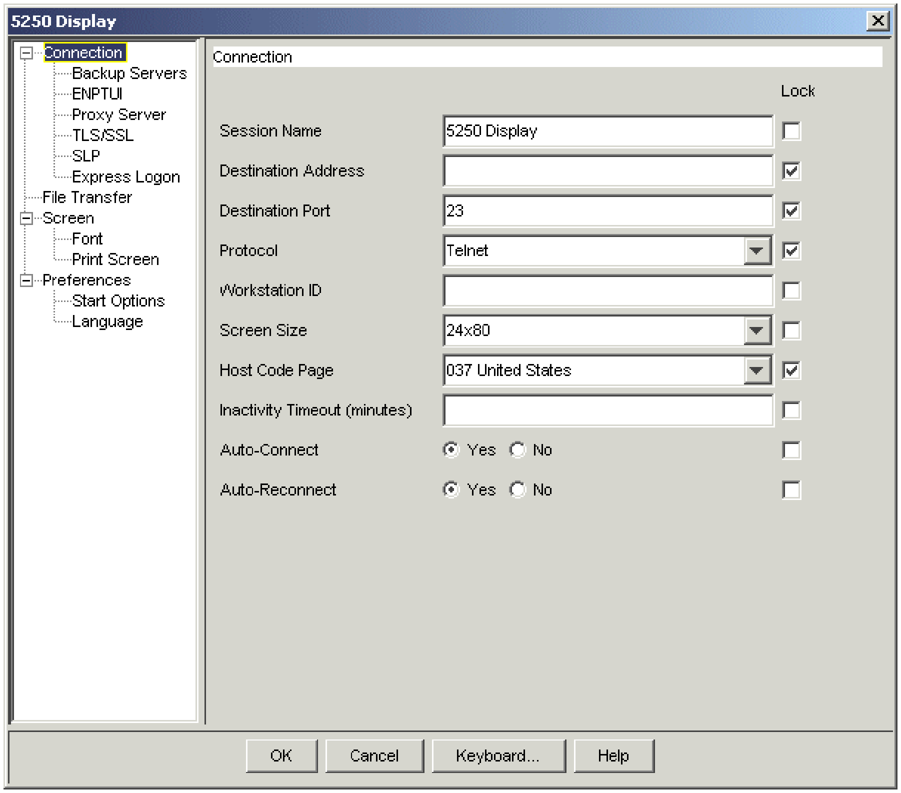


Connection

		Lock
Session Name	3270 Display	□
Destination Address		☑
Destination Port	23	☑
Protocol	Telnet	☑
TN3270E	● Yes ○ No	☑
LU or Pool Name		☑
Screen Size	24x80	□
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)		□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 7-11 3270 session Connection selection

Selecting **5250 Display** from the window shown in Figure 7-9 on page 277 brings up the window shown in Figure 7-12.



Connection

		Lock
Session Name	5250 Display	☐
Destination Address		☑
Destination Port	23	☑
Protocol	Telnet	☑
Workstation ID		☐
Screen Size	24x80	☐
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)		☐
Auto-Connect	● Yes ○ No	☐
Auto-Reconnect	● Yes ○ No	☐

Figure 7-12 5250 session Connection selection

The remainder of this section will discuss the parameters on each of the tabs.

3270/5250 Connection selection

The parameters on this selection are connection-oriented. Enter your data in the appropriate fields using the following descriptions:

- Session Name

  This is the name you wish to assign to the session. It appears beneath the session's icon and at the top of the session window. Make sure that you do not give the same name to more than one session. If you do, you run the risk of a user having sessions of the same name if he or she is a member of more than one group.

- Destination Address

  This is the host name or IP address of the Telnet server or gateway to which you want the session to connect. If the session will connect through the Host On-Demand Redirector, this must be the address of the Host On-Demand Redirector (see 6.1.10, “Redirector Service” on page 216).

  If you are configuring a Host Printing session for use as only an associated printer session, you can leave this field blank. When the associated printer session starts, Host On-Demand will use the same address used by the display session.

- Destination Port

  This is the port number on which the target server is listening for connections. If the session will connect to the Host On-Demand Redirector, this number must match the Redirector’s Local Port number defined for this connection (see 6.1.10, “Redirector Service” on page 216).

  The default port is 23 for 3270; 5250 and VT for a non-secured session; 992 for a secured session; and 2006 for CICS.

  If you are configuring a Host Printing session for use only as an associated printer session, you can leave this field blank. When the associated printer session starts, Host On-Demand will use the same port used by the display session.

- Protocol

  Select one of the following security protocols from the list:

  - Telnet

    Enables a connection between the workstation and a host server that is not secure.

  - Telnet - TLS

    Enables Transport Layer Security (TLS). TLS version 1.0 is the default security protocol for Host On-Demand clients. Note that TLS allows security negotiations from TLS version 1.0 to SSL version 3.0.

  - Telnet - SSL only

    Enables SSL version 3.0 security. Select this protocol only if the server cannot correctly negotiate a TLS connection.

- TN3270E (3270 sessions only)

  Select **Yes** if you want to enable TN3270E support. The extended TN3270 protocol (TN3270E) is required if you:

  - Want the session to connect to a specific LU or LU pool, or if you want to use an associated printer session

- Want to connect to a server in ASCII mode using the Network Virtual Terminal (NVT) protocol
- Want to use the contention-resolution mode feature of TN3270E

Support for TN3270E contention-resolution (RFC 2355) was introduced in Host On-Demand V7.02. Contention-resolution includes the abilty to negotiate usage of:

- Send Data Indicator
- Keyboard Restore Indicator
- BID Data Type and
- Signal Indicator

This allows administrators and programmers to write more accurate and efficient macros and HACL applications because they receive exact information about the status of the presentation space.

Usually a user will not notice whether the TN3270E extensions are used or not. However, after migrating to Host On-Demand V7.02 or later, users might be able to start TN3270E sessions, but will not see a logon screen. This may be caused by the fact that the TN3270 server used does not support the TN3270E contention-resolution mode. Host On-Demand V8 introduced the following parameter:

```
NegotiateCResolution = false
```

This parameter may be added to the session HTML in the Deployment Wizard to suppress the usage of the TN3270E extensions. The default value is `true`.

> **Note:** All IBM TN3270 servers support the TN3270E extensions. However, correct maintenance must be installed on Communications Server for z/OS V1.2 and higher, or COMM665 or similar hang situations can occur. Please check with your local support whether you need to migrate your server to a specific level. See 3.4, “TN3270E contention-resolution function” on page 85 for additional information.

- LU or Pool Name (3270 sessions only)

  You may want to specify the name of an LU or LU pool, defined at a Telnet TN3270E server, to which the session must connect. If you do not specify an LU or pool, the result depends on the type of server to which the session is connecting. Mostly, you will get a session from the server’s default pool. If you are connecting to Communications Server/390 V2R10 or later, you can enter the name of a LUGROUP for the POOL name.

If you enter an LUGROUP name for the pool name, this tells the Telnet server that this is a request for a specific. Communications Server/390 Telnet will check the specific LUGROUPs when selecting the LU. This requires that the SPECIFIC keyword my be added to the LUMAP statement to match the request. For example, see Example 7-1.

Example 7-1 Defining SPECIFIC LUs

```
LUGROUP HODLU
 HOD1 HOD2 HOD3 HOD4
ENDLUGROUP

IPGROUP HODIP
 0.0.0.0 : 0.0.0.0
ENDIPGROUP

LUMAP
 HODLU HODIP SPECIFIC
```

SPECIFIC pools are used to satisfy requests from clients that request a specific device name. If a specific request fails to match a device name in the SPECIFIC LU pool, the GENERIC pool will be searched.

When Enable SLP is `Yes`, this field can contain only a pool name. If a specific LU name is required (for example, for printing), do not use SLP.

If you are configuring a Host Printing session for use only as an associated printer session, this field can be left blank. When the associated printer session starts, Host On-Demand will determine the LU name from the Telnet server.

- Workstation ID (5250 sessions only)

  Defines the name of the workstation. Refer to 4.7.1, “5250 Workstation ID” on page 143 for a complete discussion of the options available. If you do not complete this field, a workstation ID is automatically defined by the host.

- Screen Size

  The number of rows and columns in the session screen. The sizes are available from a drop-down list. The default is 24x80.

- Host Code Page

  Specifies the table used to map EBCDIC codes from the host to appropriate ANSI graphics on the workstation. The default is the code page that corresponds to the locale for which your workstation is configured, but you might need to change it, for example, if the session will connect to a host system in another country. You must set it to the code page supported by the host system to which the session will connect. For many countries, the default is the Euro version of the code page; only these will support the Euro currency symbol.

- Session Inactivity Timeout (minutes)

  Specifies the number of minutes that the Host On-Demand client will wait before terminating an inactive session connection. By default, the session connection is never timed out. The session will not automatically reconnect after timing out, even if Auto-Reconnect is set to `true`.

  Terminating an idle connection may be useful for ensuring that resources such as LU names and workstation IDs are released when they are no longer being used. This option is available for 3270 or 5250 display/print sessions, or VT sessions only.

- Auto-Connect

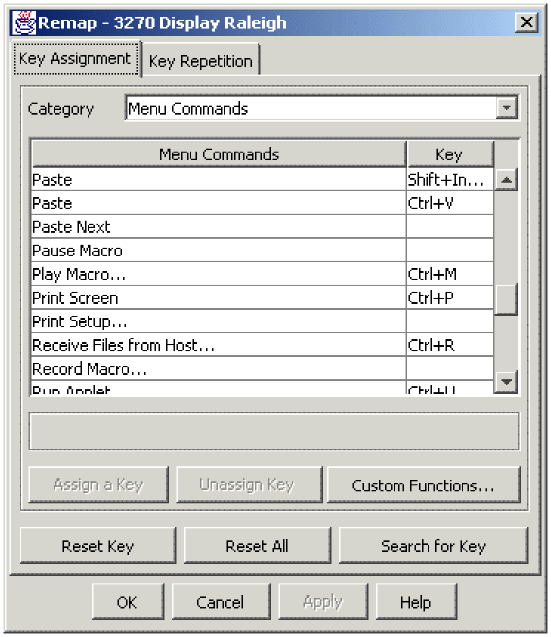
  Specifies whether the session should be automatically connected to the target Telnet server. If you set this to `No`, you must click **Connect** in the session menu every time you want to connect a session.

- Auto-Reconnect

  Reconnects the session automatically if communication fails and later recovers.

- Keyboard button

  Click the keyboard button at the lower end of the session definition window to see the keyboard remap window as shown in Figure 7-13. Using this feature, you can assign keys or key combinations as “shortcuts” to functions or applets. For example, you could assign Ctrl+m to execute a menu command, or Alt+a to run an applet. Walk through the available Categories by clicking the drop-down menu for that and viewing the assignments of the keys. The example shows the Category Menu Commands, which contains for example, the mapping for the cut and paste functions. Please view those examples and use the online help for this panel to understand to this utility.



Category: Menu Commands

Menu Commands	Key
Paste	Shift+In...
Paste	Ctrl+V
Paste Next	
Pause Macro	
Play Macro...	Ctrl+M
Print Screen	Ctrl+P
Print Setup...	
Receive Files from Host...	Ctrl+R
Record Macro...	
Run Applet	Ctrl+U

Figure 7-13 Keyboard remapping

- Lock

  You can select **Lock** for any configurable parameter to prevent users from changing the associated startup value for that session. However, functions accessed from the session menu bar or tool bar can be changed. The lock option is available on all tabs of all sessions.

3270 Associated Printer selection

You can associate a 3270 printer session with a 3270 display session. Make sure the association has been correctly configured at the Telnet server.

- Associated Printer Session (3270 sessions only)

  TN3270E lets you associate a 3270 printer session with a 3270 display session. More information on associated printer sessions can be found in 21.3, “3270 Associated Printer Sessions” on page 735.

- Close Printer with Session (3270 sessions only)

  This option is enabled only when an Associated Printer Session is selected. The default is No, enabling the printer session to be connected or disconnected independently of its associated display session.

  If **Yes** is selected, the display session controls whether the printer session is connected or disconnected. The menu options to connect or disconnect are disabled in the printer session. When the display session is disconnected, the printer session is disconnected. When the display session is connected, the printer session is connected. The printer window is closed when the display session window is closed. The printer window can also be closed independently, but the display window must be closed and restarted to restart the printer session.

  When **Yes** is selected, the Session Inactivity Timeout for the printer session is ignored. When the display session times out, both the display and printer sessions are disconnected. If there is a job printing, the display and printer sessions are not disconnected until the print job completes.

  When **Yes** is selected, the settings for the Auto-Connect and Auto-Reconnect on the printer session are derived from the associated display session, regardless of their configuration in the printer session. If Auto-Reconnect is set to `No`, and the display session is disconnected by the Telnet server or because of a network problem, the printer session will also be disconnected. If Auto-Reconnect is set to `Yes` and the display session is disconnected by the Telnet server or because of a network problem, the printer session will remain connected until the display session is reconnected. If the display session LU is not associated with the running printer session LU, the printer session will be disconnected and reconnected to the display's associated printer LU.

  It is recommended that you set this to `Yes` if the Telnet server is configured to use pooled associated LUs to ensure the printer and display LUs remain in sync.

5250 ENPTUI selection

Enhanced Non-Programmable Terminal User Interface (ENPTUI) enables an enhanced user interface on non-programmable terminals (NPT) and programmable work stations (PWS) over the 5250 full-screen menu-driven interface.

- Enable ENPTUI

  Enables Enhanced Non-Programmable Terminal User Interface (ENPTUI) support.

- Enable Unicode Data Stream

  This setting enables Unicode support for OS/400. The Host On-Demand 5250 Display session displays Unicode characters that the iSeries host has written into fields tagged with a Coded Character Set Identifier (CCSID). For more information see *Unicode support for OS/400 using Coded Character Set Identifiers.*

- Lock

  Check **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

3270/5250 backup servers selection

Host On-Demand Version 8 supports definition of up to two optional backup servers for each session.These are used in the event of a failure to connect with the main server either:

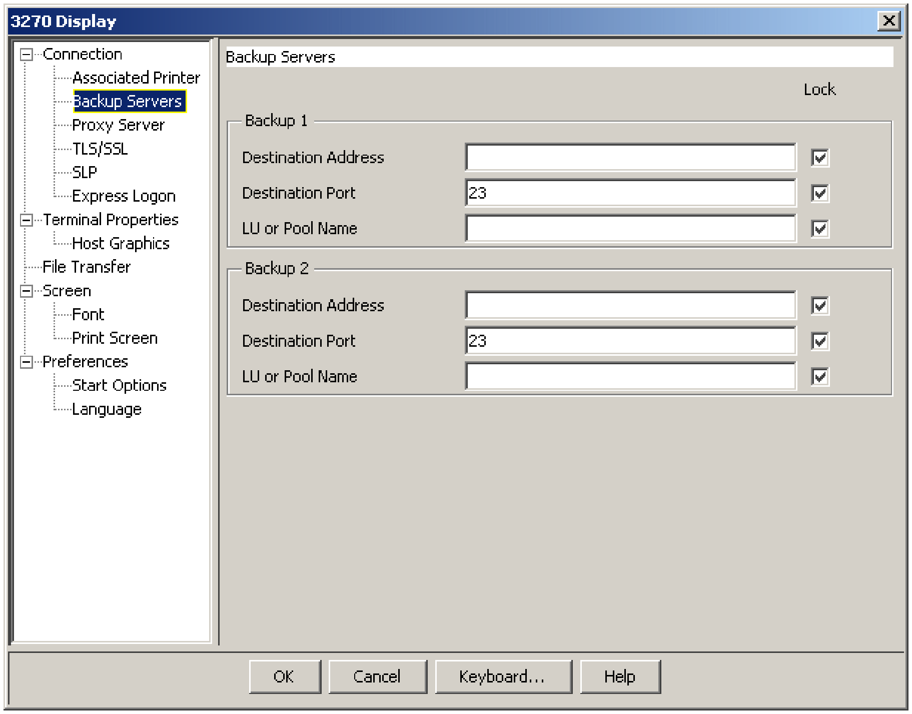
- When you first open the session; or
- During an active session after a connection failure, if you have Auto-Reconnect selected on the Advanced panel.

In either of these situations, Host On-Demand will always try connecting with servers in the following order:

- The main server (the server specified in the Destination Address field of the Connection selection).
- Backup 1, if the attempt to connect with the main server fails and Backup 1 is specified.
- Backup 2, if the attempt to connect with Backup 1 fails and Backup 2 is specified.

Failure to connect with a particular server may occur because the server does not exist, because the server is unreachable, or because the server is not answering. When Enable SLP is **Yes**, all the fields on this panel are disabled. Backup servers are available with the following session types: 3270 Display, 3270 Printer, 5250 Display, 5250 Printer, CICS Gateway client, and VT Display.

Each definition for a backup server consists of Destination Address, Destination Port and LU Pool Name. See Figure 7-14.



Backup Servers

Lock

Backup 1

Destination Address ☑

Destination Port 23 ☑

LU or Pool Name ☑

Backup 2

Destination Address ☑

Destination Port 23 ☑

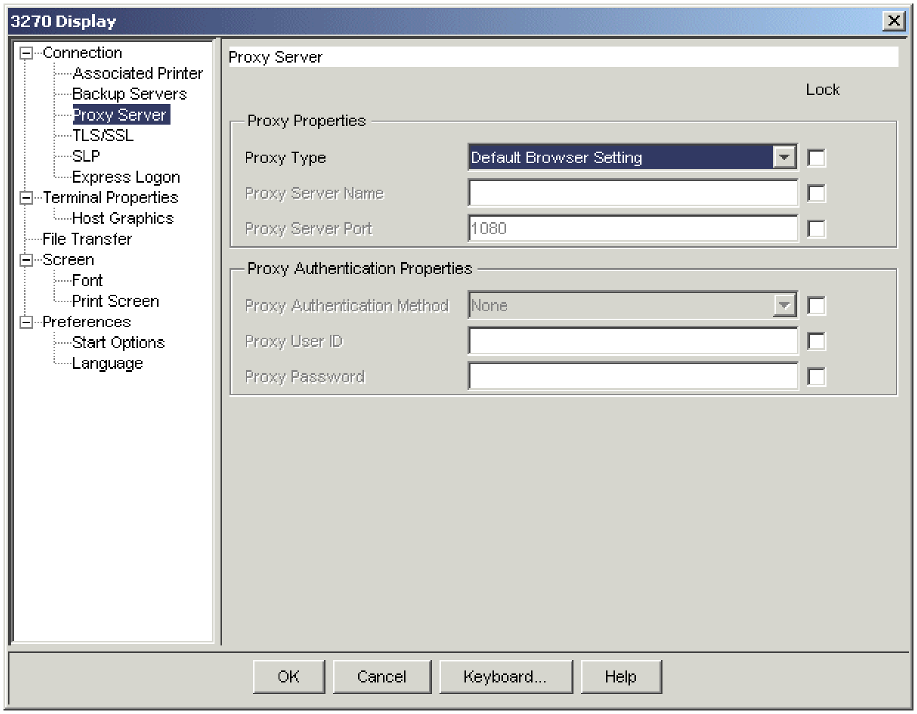
LU or Pool Name ☑

Figure 7-14 Defining backup servers

For a description of these parameters see “3270/5250 Connection selection” on page 280.

3270/5250 Proxy Server selection

A Host On-Demand session can connect to a host system through a proxy server, which enables applications to communicate transparently across a firewall. The proxy server connects to the host on behalf of the Host On-Demand session, and relays data between the session and the host system.



Proxy Server

Lock

Proxy Properties

Proxy Type	Default Browser Setting	□
Proxy Server Name		□
Proxy Server Port	1080	□

Proxy Authentication Properties

Proxy Authentication Method	None	□
Proxy User ID		□
Proxy Password		□

Figure 7-15 3270/5250 Proxy Server selection

- Proxy Properties
  - Proxy Type

    A Host On-Demand session can connect to a host system through a proxy server. A proxy server enables applications to communicate transparently across a firewall. The proxy server connects to the host on behalf of the Host On-Demand session, and relays data between the session and the host system.

    This field allows you to specify what type of proxy server a host session uses. Select one of the following:

    - Default Browser Setting

      The session uses the proxy settings of the Web browser where the session runs.

      The Java Virtual Machine (JVM) used in many Web browsers supports only Socks Version 4 connections. If your proxy server supports Socks Version 5, and you wish to use all of its features (such as authentication and enhanced IP address support), do not use the default browser settings. Instead, select **Socks V5** as the proxy type.

  - HTTP Proxy

    The session only connects through an HTTP proxy server, overriding the proxy settings defined in the Web browser.

  - Socks V4

    The session only connects through a Socks Version 4 proxy server, overriding the proxy settings defined in the Web browser. A Socks Version 4 proxy server connects to a host system on behalf of a Host On-Demand client, and transmits data between the client and the host system.

  - Socks V5

    The session only connects through a Socks Version 5 proxy server, overriding the proxy settings defined in the Web browser. Socks Version 5 includes the complete functionality of Socks Version 4; in addition, it supports authentication to the proxy server, IP Version 6 addressing, domain names, and other networking features.

  - Socks V4 if V5 unavailable

    The session first attempts to connect using Socks Version 5. However, if the proxy server does not support Socks Version 5, the session connects using Socks Version 4. In either case, the session overrides the proxy settings defined in the Web browser.

The following field is unavailable if **Use Default Browser Setting** is selected as the proxy type:

- Proxy properties

  If the session is connecting to the host system through a Socks or HTTP proxy server, set the proxy server properties as follows:

  - Proxy Server Name

    Enter the hostname or IP address of the Socks or HTTP proxy server.

  - Proxy Server Port

    Enter the TCP port number of the Socks or HTTP proxy server.

  The following fields are available only if **HTTP Proxy**, **Socks V5** or **Socks V4 if V5 unavailable** is selected as the Proxy Type, and **Base** respectively **Clear text** is selected as the Proxy Authentication Method.

  - ProxyUser ID

    Type the user ID that the Host On-Demand session provides to authenticate with the HTTP or Socks proxy server.

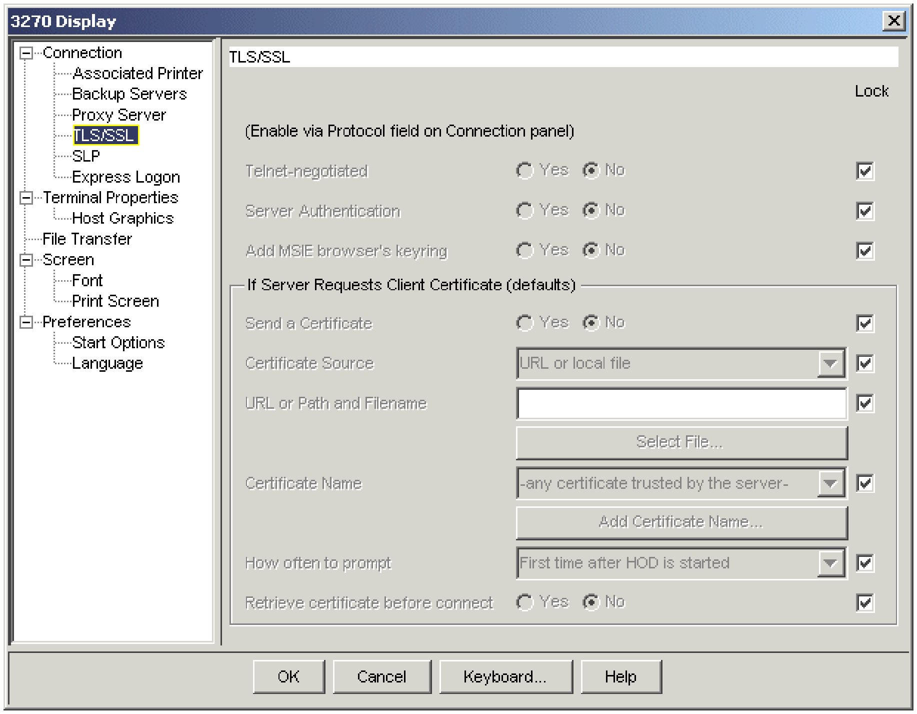
– Proxy Password

Type the password that the Host On-Demand session provides to authenticate with the HTTP or Socks proxy server.

> **Note:** If the HTTP or Socks proxy server requires a user ID and password, and you do not enter them here, the server will prompt you for them at connection time.

3270/5250 TLS/SSL selection

The TLS/SSL selection specifies the options required to establish secure sessions. The 3270 session has additional parameters for the security protocol and Telnet negotiation.



TLS/SSL

Lock

(Enable via Protocol field on Connection panel)

Telnet-negotiated ○ Yes ● No ☑

Server Authentication ○ Yes ● No ☑

Add MSIE browser's keyring ○ Yes ● No ☑

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No ☑

Certificate Source: URL or local file ☑

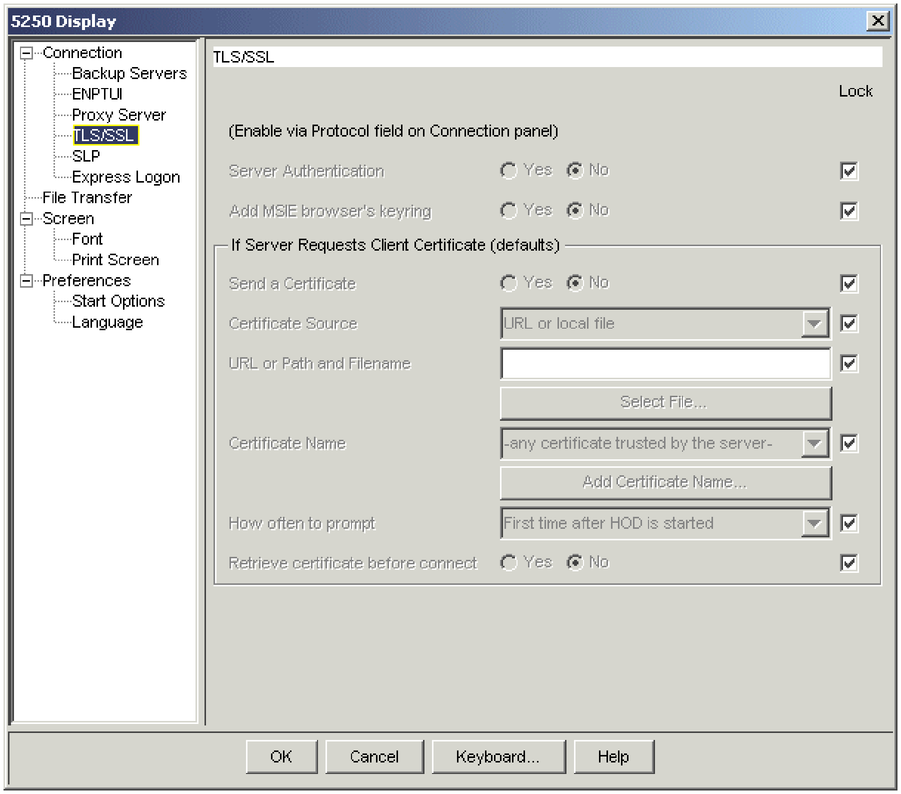
URL or Path and Filename: ☑

Certificate Name: -any certificate trusted by the server- ☑

How often to prompt: First time after HOD is started ☑

Retrieve certificate before connect ○ Yes ● No ☑

Figure 7-16 3270 session TLS/SSL selection



TLS/SSL

Lock

(Enable via Protocol field on Connection panel)

Server Authentication ○ Yes ● No ☑

Add MSIE browser's keyring ○ Yes ● No ☑

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No ☑

Certificate Source: URL or local file ☑

URL or Path and Filename: ☑

Select File...

Certificate Name: -any certificate trusted by the server- ☑

Add Certificate Name...

How often to prompt: First time after HOD is started ☑

Retrieve certificate before connect ○ Yes ● No ☑

Figure 7-17 5250 session TLS/SSL selection

Additional information on session configuration for security can be found at 11.4, “Defining a secure Telnet session” on page 427.

If the function has been enabled using the protocol field at the Connection selection, the following parameters can be used to define the session security.

- Telnet-negotiated

  Determines whether the security negotiations between the client and the Telnet server are done on the established Telnet connection or on a TLS connection prior to the Telnet negotiation. For the client to use this feature, the Telnet server must support TLS-based Telnet Security. The other options are valid regardless of whether Telnet-negotiated is set to `Yes` or `No`.

- Server Authentication

  Ensures that a secure session is established only if the Internet name of the server matches the common name in the server's certificate. This is effective only on a locally-installed client or a client downloaded through HTTPS.

- Add MSIE Browser's Keyring

  When this option is selected, the Host On-Demand client accepts Certificate Authorities trusted by the Microsoft Internet Explorer browser.

The following options are used to specify the handling of client authentication.

- Send a Certificate

  Enables Client Authentication. If this option is turned off and the server requests a client certificate, the server will be told that no client certificate is available, and the user will not be prompted.

- Certificate Source

  Once **Send a Certificate** is selected, this field is enabled. The client certificate can be kept in either a URL or local file or in the client's browser or a dedicated security device such as a smart card.

  Alternatively, it can be kept in a local or network-accessed file, in PKCS12 or PFX format, protected by a password.

- URL or Path and Filename

  Specifies the default location of the client certificate. The URL protocols you can use depend on the capabilities of your browser. Most browsers support HTTP, HTTPS, FTP, and FTPS.

- Select File

  You may optionally click **Select File** and browse the file system available to the local system to locate the certificate.

- Certificate Name

  This drop-down menu is enabled if you indicate that the certificate is located in the browser or a security device. It lists all personal certificates found in the Microsoft cryptographic database. Optionally, you may choose to accept **“-any certificate trusted by the server-”**.

- Add Certificate Name

  This button invokes a dialog to specify the parameters for choosing a client certificate, including the common name, e-mail address, organizational unit, and organization used to define it (this button is only available on the administrator's configuration panel).

- How often to prompt

  This drop-down menu allows you to control the timing of prompts for client certificates. You can choose to prompt each time a connection is made to the server, or only the first time after starting HOD.

If your certificate is in a password-protected file and your client supports storing preferences locally, choosing **Prompt only once** causes HOD to prompt for the password the next time the connection is made, but never after that, unless the connection attempt fails.

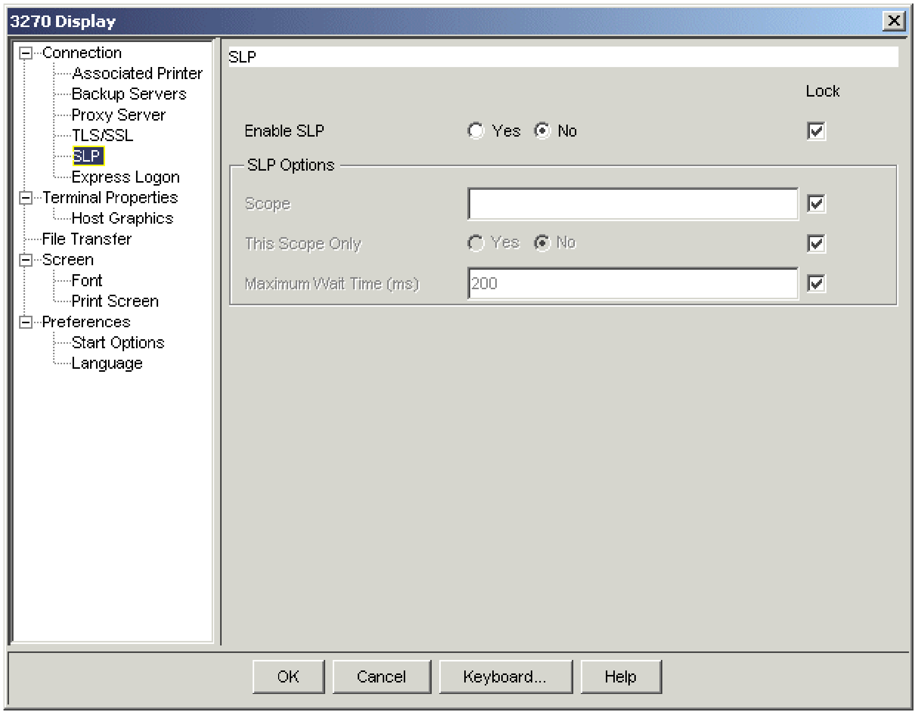
If your certificate is accessed through the MSIE browser, **Prompt only once** can be chosen on any client, as well as **Do not prompt**, which will disable the prompt from HOD, but not from the browser or security device.

- Retrieve certificate before connecting

  If this is turned on, the client will access its certificate before connecting the server, whether the server requests a certificate or not. If this is turned off, the client will only access the certificate after the server has requested it; depending on other settings, this may force the client to abnormally terminate the connection to the server, prompt the user, and then re-connect.

3270/5250 SLP selection

Service Location Protocol (SLP) enables a client to dynamically locate a TN3270 and TN5250 service, and to attach to the least-loaded server, making it unnecessary for you to know the destination address and port of any specific service. For more details on SLP, refer to Appendix B, “Service Location Protocol” on page 1049.



SLP

		Lock
Enable SLP	○ Yes ● No	☑

SLP Options

Scope		☑
This Scope Only	○ Yes ● No	☑
Maximum Wait Time (ms)	200	☑

Figure 7-18 3270/5250 session SLP selection

- Enable SLP

  This enables you to dynamically find a service without knowing the destination port and address. Your network must be configured to support the Service Location Protocol (SLP). If SLP is supported in the network, Host On-Demand will connect to the server that responds with the least session load. If Enable SLP is `Yes`, there is no way to specify a specific LU name when establishing a connection, so you can use only pool names.

- AS/400 Name (SLP) (5250 Session only)

  Connects a session to a specific iSeries. Type the fully-qualified SNA CP name; for example, `USIMBNM.RAS400B`. If you do not specify an SLP iSeries name, the session connects to the default iSeries defined at the server. This field is available only when Enable SLP is set to `Yes`.

  The first character must be A through Z, $ (dollar sign), @ (commercial at sign), or # (number sign). The remaining characters can be A through Z, 0 through 9, $, @, or #.

- SLP Options

These fields control and manage the access by TCP/IP clients to servers that support SLP.

- Scope

  Controls and manages access by TCP/IP clients to servers that support SLP. Contact your administrator to get the correct value for this field.

  If a server is not found within the specified scope, the session can be established only through an unscoped server; however, if this scope is set to `Yes`, the session will connect only if a server with that scope is located.

  The default is blank and this returns all scoped and unscoped services depending on the level of the Communications Server you are running.

  We recommend that you configure all of your servers with scopes.

  Special characters , (comma), / (forward slash), and : (colon) are not allowed in the Scope field.

- This Scope Only

  Prevents a session from connecting to an unscoped server. If you set this to `Yes` and no server is found within the specified scope, the session will not connect.

  The default is No.

- Maximum Wait Time (slp)

  Sets the maximum time, in milliseconds, that the session waits to discover services or directory agents, or responses concerning load information. This value must be greater than zero and less than 3600000ms (1 hour).

  The default is 200.

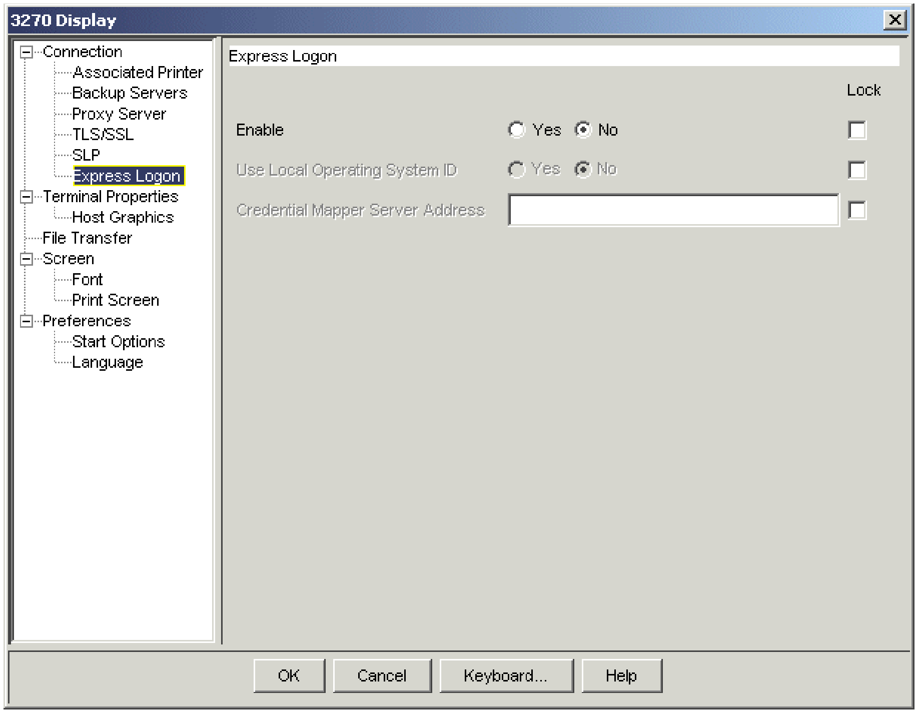
  Directory Agent Discovery timeout and Service Agent Multicast timeout are both set with this value.

- Lock

  Select **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

3270/5250 Express Logon selection

Web Express Logon provides an automated way for users to logon to hosts and host-based applications without having to provide an additional user ID. Refer to Chapter 15, “Express Logon” on page 555 for more details on Express Logon.



Enable ○ Yes ● No ☐

Use Local Operating System ID ○ Yes ● No ☐

Credential Mapper Server Address ☐

Figure 7-19 3270/5250 session express logon selection

- Enable

  Select Yes to enable Web Express Logon. The default is No.

- Use Kerberos Passticket (5250 sessions only)

  Click Yes for Host On-Demand to retrieve a Kerberos Passticket from a Windows 2000 or Windows XP operating system. This Passticket is used to connect to the host system that you identify in the session properties. This type of authentication does not make use of macros.

- Use Local Operating System ID

  Click Yes to allow Host On-Demand to use the user's local operating system ID for authentication.

- Credential Mapper Server Address

  Type the full URL of the Credential Mapper Server, for example, https://server_name/junction/cm/CredMapper, where server_name is the name of the authentication server, junction is the name of the junction (this may be optional, depending on your network security application), cm is the Credential Mapper application space and CredMapper is the servlet name.

The servlet that resides at this URL processes the HTTPS request from the user, performs a lookup, and returns the user's credentials. The Host On-Demand client uses the obtained credentials to automate the login process.

3270 Terminal Properties selection

This selection provides additional session functions.

Reset Insert Mode on Aid Key

If **Yes** is selected and you are in insert mode, then any aid key will turn the insert mode off. If enabled and you are not in insert mode, this function has no effect on the operation of the aid key. An aid key is an attention identifier key, any key that causes an interrupt to be sent to the host application, such as Enter, PF keys, or PA keys.

3270 Host Graphics selection

This selection provides additional session functions.

Enable Host Graphics

Enables the 3270 host graphics function. If this is enabled, Character Cell Size will specify the cell characteristics used for host graphics. The default is No.

3270/5250 File transfer selection

The file transfer function allows to copy files from the host to your workstation or from your workstation to the host.

- File Transfer Type

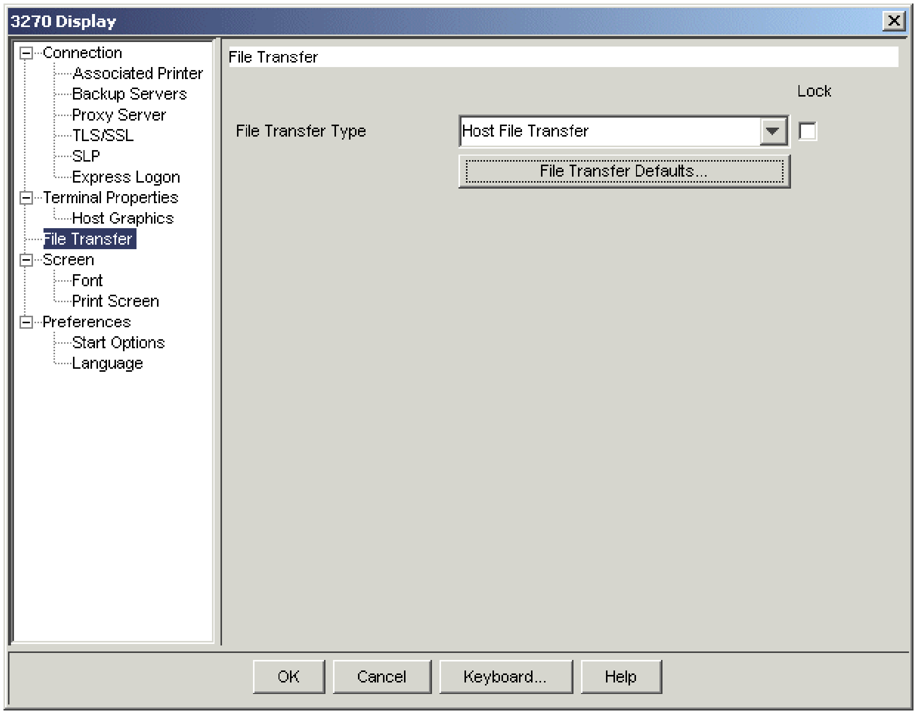
  Determines whether the file transfer type is Host File Transfer or FTP. If the File Transfer Type is FTP, a separate FTP session is started from the display session.

Important: An integrated FTP session does not inherit the security properties of the display session. At configuration time, a warning message will appear, if the administrator tries to configure a secured FTP-session to a unsecured display session.

- File Transfer Defaults

  The 3270 host file transfer is implemented by using the IND$FILE host program to transfer files through the 3270 data stream in DFT mode. In the General tab of the 3270 file transfer, you select which is your default host type used for file transfer.

For example, if you have in your company environment only hosts using VM, you select in the General tab for Host Type the **VM/CMS** from the drop-down menu. After that, you configure your VM/CMS preferences using the VM/CMS tab. An example is shown in Figure 7-21 on page 300. Your users can start the file transfer from their 3270 session without needing to change or configure it.

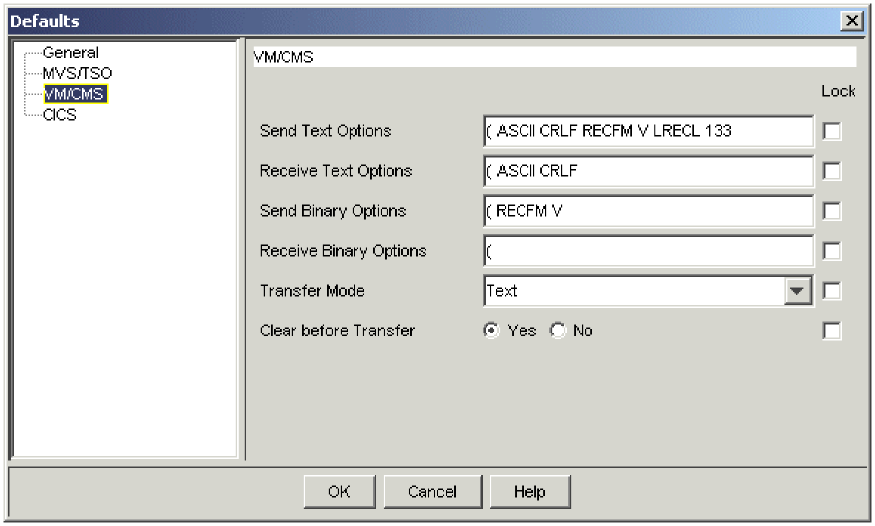


File Transfer

Lock

File Transfer Type: Host File Transfer ☐

Figure 7-20 3270 file transfer selection



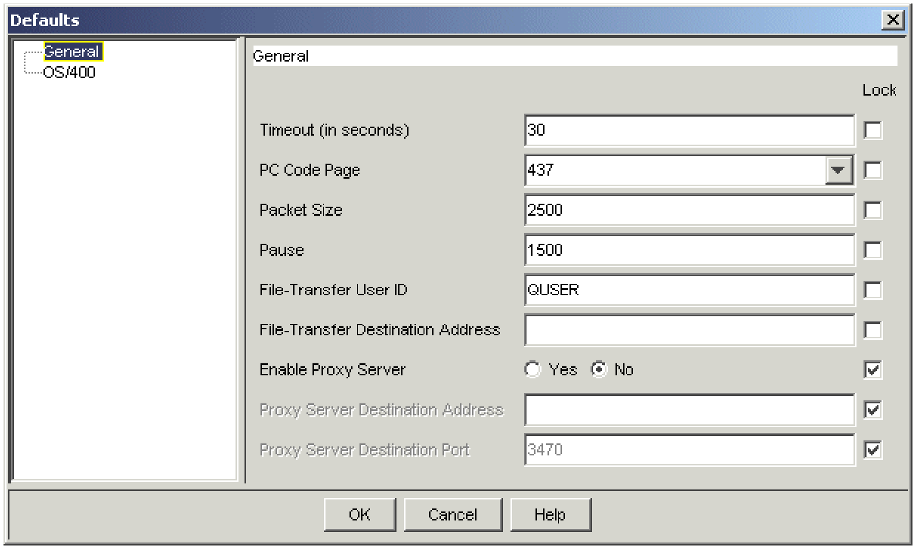
VM/CMS

		Lock
Send Text Options	(ASCII CRLF RECFM V LRECL 133	□
Receive Text Options	(ASCII CRLF	□
Send Binary Options	(RECFM V	□
Receive Binary Options	(	□
Transfer Mode	Text	□
Clear before Transfer	● Yes ○ No	□

Figure 7-21 Example of VM/CMS file transfer settings

If you have more than one host type with which users have to exchange data, you can configure the preferences for each host type. But do not lock the Host Type in the General window, so that the user can change it (the user has to switch the host type using **Actions -> File Transfer Defaults** to select the host type to which he transfers data). For more details, refer to the online help.

If **FTP** is selected, refer to “FTP/sftp session” on page 322 for an explanation of the configuration.



General

		Lock
Timeout (in seconds)	30	□
PC Code Page	437	□
Packet Size	2500	□
Pause	1500	□
File-Transfer User ID	QUSER	□
File-Transfer Destination Address		□
Enable Proxy Server	○ Yes ● No	☑
Proxy Server Destination Address		☑
Proxy Server Destination Port	3470	☑

Figure 7-22 5250 host file transfer

In the 5250 file transfer window, the defaults will vary depending upon what file transfer type is selected, Host File Transfer or FTP.

If **Host File Transfer** is selected, you will see the window shown in Figure 7-22 on page 301. For details, refer to online help.

If **FTP** is selected, refer to “FTP/sftp session” on page 322 for an explanation of the configuration.

3270/5250 Screen selection

These parameters change the look of the session data.

- Alternate Terminal

  Causes Host On-Demand to format the session window so that it looks like a traditional graphical user interface (with icons, buttons, text input fields, and so on) rather than like a traditional host “green screen” (green characters on a black background).

  Click Enabled if you want to use the Alternate Terminal interface.

  Click Disabled if you do not want to use the Alternate Terminal interface.

- Cursor Style

  Determines whether the cursor displays as an underscore or a block while the keyboard is in Replace mode. You can also click **Altcur** on the session-window keypad to change the cursor style.

- Light Pen Mode

Choose to switch Light Pen Mode on or off when the session starts. Some host applications use a light pen as a pointer and operator. If you switch light pen mode on, you can use your mouse as a light pen.

The default is No (off).

3270/5250 Font selection

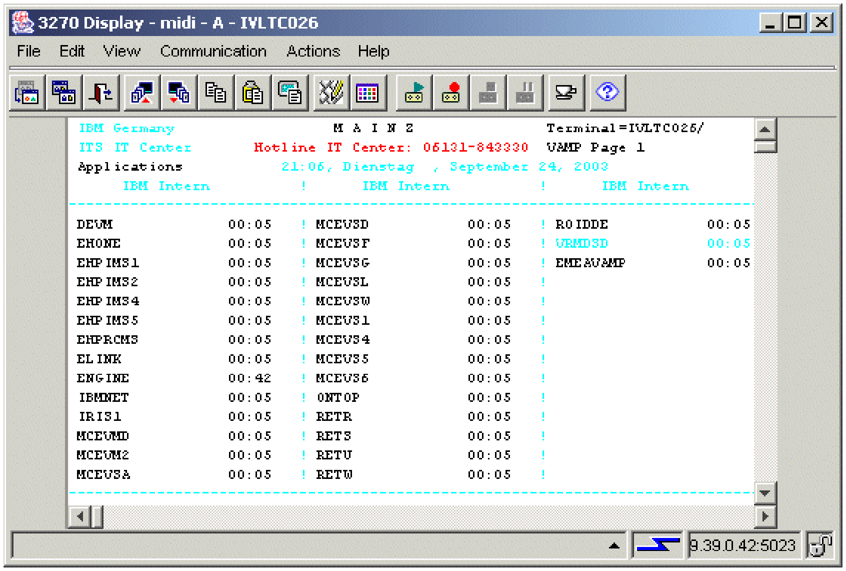
These parameters change the look of the session data and as a result also the behavior of the session window.

- Fixed Font

  A font that, when applied to screen display characters, never changes in size, despite manipulations of the active display window.

  Select Yes to apply a fixed font to your display. (Remember that when you select Fixed Font and resize your display window to smaller dimensions, you only shrink your view of the display. The display contents remain the same size.)

  Select No to enable the font of your display characters to resize dynamically as you manipulate the active display window.



```
IBM Germany                      M A I N Z              Terminal=IVLTC026/
ITS IT Center          Hotline IT Center: 06131-843330  VAMP Page 1
Applications              21:06, Dienstag  , September 24, 2003
     IBM Intern           !       IBM Intern           !      IBM Intern
--------------------------------------------------------------------------------
DEVM              00:05   ! MCEVSD            00:05   ! ROIDDE            00:05
EHONE             00:05   ! MCEVSF            00:05   ! VRMDSD            00:05
EHPIMS1           00:05   ! MCEVSG            00:05   ! EMEAVAMP          00:05
EHPIMS2           00:05   ! MCEVSL            00:05   !
EHPIMS4           00:05   ! MCEVSW            00:05   !
EHPIMS5           00:05   ! MCEVS1            00:05   !
EHPRCMS           00:05   ! MCEVS4            00:05   !
ELINK             00:05   ! MCEVS5            00:05   !
ENGINE            00:42   ! MCEVS6            00:05   !
 IBMNET           00:05   !  ONTOP            00:05   !
 IRIS1            00:05   ! RETR              00:05   !
MCEVMD            00:05   ! RETS              00:05   !
MCEVM2            00:05   ! RETU              00:05   !
MCEVSA            00:05   ! RETW              00:05   !
--------------------------------------------------------------------------------
```

Figure 7-23 Fixed font emulator window with scroll bars (Java 2)

- Fixed Font Size

  Select the desired font size from the drop-down menu.

- Font Name

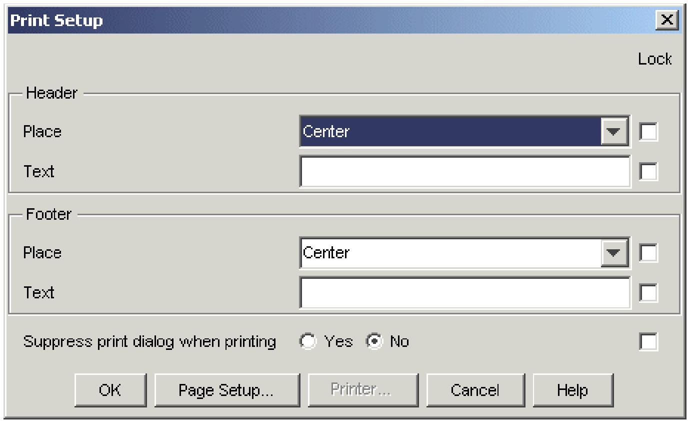
The type of font used to display characters on the screen. The choices are: Monospaced, Courier, IBM3270, ARB3270 (Arabic), HEB3270 (Hebrew) and THA3270 (Thai). The 3270 fonts are very similar to the sans-serif default font used by Personal Communications. The default is Monospaced.

- Font Style

  You can choose between Plain, Italic or Bold. The default is Plain.

3270/5250 Print Screen selection

To print a terminal emulator session screen, click Print Screen Setup (Java 2). You will see the panel shown in Figure 7-24.(Remember that you can only print screens to printers installed on your desktop.)



Header

Place: Center □

Text: □

Footer

Place: Center □

Text: □

Suppress print dialog when printing ○ Yes ● No □

Figure 7-24 3270/5250 session Print Screen setup

- Header or Footer

  Lets you specify the text of a header or footer that appears at the top or bottom margin of a printed screen.

  – Place

    The horizontal alignment of the header or footer. Can be one of the following:

    - Left
    - Right
    - Centered

  – Text

The header or footer text. Headers can include automatically updated page numbers, dates, times, and so forth; see the help for a complete list. When Alternate Terminal is enabled, the print preview function does not show header or footer text.

- Suppress print dialog when printing

  Select Yes to suppress the display of the Print dialog when you print a screen. The Print dialog will only appear when you first print a screen, to enable you to set printer attributes.

  Select No to have the Print window appear every time you print a screen.

- Page Setup

Click this button to display the Page Setup window, enabling you to specify the paper type, page orientation and margins for your printouts.

During an active session, choose File > Print Screen Setup > Print Setup to access the following options

- Suppress print dialog when printing
- Printer
- Page Setup

The Print Setup and Page Setup options are only applicable to browsers that support Java 2.

3270/5250 Preferences selection

The Preferences selection for 3270 and 5250 Display Sessions reflects operational characteristics of the session:

- Confirm on Exit

  Select **Yes** if you want a warning message to appear when a user attempts to close a session. If users select **File -> Exit**, close a session window, exit from the toolbar, or right-click the left corner of the session window, a window appears asking if they really want to exit. If the user clicks **OK**, the session ends. If the user clicks **Cancel** or closes the window, the session remains open and unchanged. If the user closes the browser window, no exit warnings appear. If the user closes both a session and its associated printer session, the exit warning appears only once.

  The default is No.

- Show Border

  Sets the border color around a session to either gray or black. If the background color of the session is black, the session appears to have no border. The default is Yes (gray border around the session).

- Graphical OIA

  Determines whether the Graphical Operator Information Area (OIA) is visible on the screen. The default is Yes (visible).

- Textual OIA

  Determines whether the Textual OIA is visible on the screen.The default is No (not visible).

- Keypad

  Determines whether the Keypad is visible on the screen. You can also turn this on or off from the View menu in the session screen.

  The default is No (not visible).

- Toolbar

  Determines whether the Toolbar is visible on the screen. You can also turn this on or off from the View menu in the session screen.

  The default is Yes (visible).

- Toolbar Text

  Determines whether the text that explains the purpose of each toolbar button is visible on the toolbar buttons. You can also turn this on or off from the View menu in the session screen.

  The default is No (not visible).

- Status Bar

  Determines whether the Status Bar is visible at the bottom of the screen when the session starts. The Status Bar displays connection status messages and toolbar button descriptions. You can also turn this on or off from the View menu in the session screen.

  The default is Yes (visible).

- Macro Manager

  Determines whether the Macro Manager toolbar is visible on the screen. You can also turn this on or off from the View menu in the session screen.

  The default is No (not visible).

3270/5250 Start Options selection

The Start Options selection for 3270 and 5250 Display Sessions reflects operational characteristics related to the start of the session.

- Session ID

ID assigned to this session, A-Z. Sessions are started in alphabetical order. Automatic assigns the next available capital letter to the session. You may wish to assign a specific session ID if you have an HACL applet or EHLLAPI program that requires a specific session ID; otherwise, we recommend you select the **Automatic** setting.

- Start Automatically

  If **Yes** is selected, the session is started and connected (if Auto-Connect is Yes) when the client is loaded.

- Start in Separate Window

  Specifies whether the session is started in a separate browser window. If `No`, the session is started in the Client window with the session name and ID displayed on a tab. Each session started in the Client window is tabbed for easy access.

- Auto-Start Applet/Macro Options

  - Auto-Start

    Specifies whether an applet or macro should be run when the session is started.

  - Auto-Start name

    Specifies the name of the applet or the macro to be run when the session starts.

  - Parameter (Optional)

    The name of the parameter that is passed to the applet when the session starts. In order for an applet to receive parameters, the applet must implement the following method: public void initParam(String param). The variable name, param, may be any valid variable name.

3270/5250 Language selection

The following section describes the contents of the Language selection for 3270 and 5250 sessions. The fields on this page will not be enabled unless the code page of the system supports this page, such as Arabic, Hebrew, Thai, Chinese, Japanese or double-byte character set users.

- Edit Bidi options

  - Numeral Shape (Arabic only)

    Determines the shape of numeric characters of the string copied to or pasted from the clipboard. You have a choice between Nominal, National, or Contextual.

    The default is Nominal.

  - Text Type (Arabic and Hebrew only)

  Determines the format of the text that is copied to or pasted from the clipboard. You have a choice between Visual or Logical.

  The default is Visual.

  - Text Orientation (Arabic and Hebrew only)

    Determines whether the orientation of characters copied to or pasted from the clipboard is left-to-right or right-to-left.

    The default is Left-to-Right.

  - Round Trip (Arabic and Hebrew 5250/3270 only)

    The Round Trip option disables the reversal of numerals if preceded by Bidi characters in the text copied to or pasted from the clipboard.

    The default is On.

- Display Bidi options

  - Allocate space for LamAlef (Arabic 5250 only)

    This option is to protect the LamAlef character at the Implicit file on iSeries systems. When this option is On, each LamAlef will allocate space at the end of the Arabic field.

    The default is Off.

  - Numeral Shape (Arabic VT only)

    Determines the shape of numeric characters on the screen. You have a choice between Nominal, National, or Contextual.

    The default is Contextual.

  - Text Type (Hebrew VT only)

    Determines the format of the text characters stored. You have a choice between Visual or Logical.

    The default is Visual.

  - BIDI Mode (Arabic VT only)

    Sets text display and cursor behavior to support VT display settings.

    The default is On.

  - Cursor Direction (Hebrew Visual VT only)

    Sets the cursor direction left-to-right (LTR) or right-to-left (RTL). When cursor direction is set RTL, all characters are displayed in the RTL direction because the cursor moves left by default after each displayed character. In general, only applications that are designed to receive input in a RTL direction will work properly when the Cursor Direction is set to `RTL`.

The default is LTR.

- Smart Ordering (Arabic/Hebrew Logical VT only)

  Determines whether segments of characters with different text attributes are ordered separately.

  The default is Off.

- Show Text Attributes (Arabic/Hebrew Logical VT only)

  Enabled only when Smart Ordering is set to `On`.

  The default is Yes.

- Print RTL file (Arabic and Hebrew 3270 Printer session only)

  Select **Yes** to print a file as it appears on a RTL screen. Print RTL file is available only for printing to Windows printers or Adobe PDF files.

  The default is No.

- Thai options

  - Thai Display Mode

    Select a display mode:

Table 7-1 Display modes

Mode	Description
1 - Non-compose	No character composition occurs
2 - Composed	Thai characters are auto-composed. No column realignment is performed.
3 - Composed with space alignment	Three consecutive spaces cause column realignment. The realignment occurs whenever composing routine finds three consecutive spaces. If all fields have at least three trailing spaces, then all fields of all records will be properly aligned.
4 - Composed with EOF alignment	The EOF character (Hexadecimal 'EA') also causes column realignment. Whenever the composing routine finds a single EOF, it deletes the EOF and performs column realignment. If two consecutive EOFs are found, no realignment occurs, one EOF is deleted, and one EOF is treated as data.
5 - Composed with space and EOF alignment	Combines column realignment function of both mode 3 and mode 4.

- Lock

Select **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

- DBCS options
  - User Defined Character Setting

    Determines whether the session starts with a user-defined character (UDC) mapping table.

    The default is Off. If you want to use a UDC mapping table, set this option to `On`.
  - UDC Table Selection

    Select the UDC mapping table that will be applied in this session. You can create a new mapping table.

    The default is None.
  - IME Auto Start

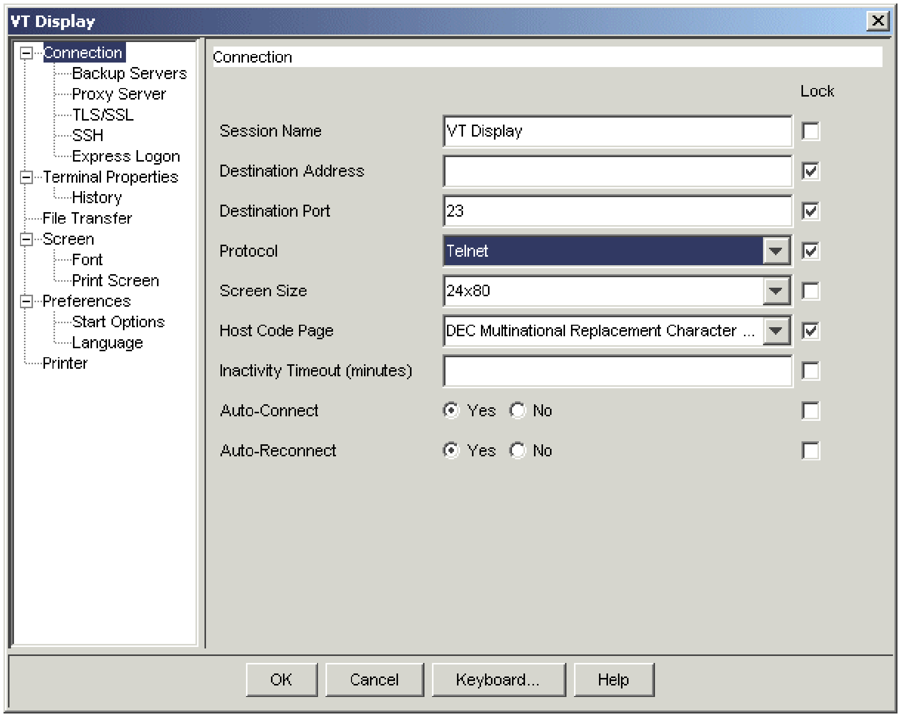
    Select **Yes** to automatically start the Input Method Editor (IME) when the cursor is located on DBCS fields. IME is a front-end processor that generates DBCS strings. This function requires Java 2.

    For DBCS sessions running on Java 2, the default is On. For all other sessions, the default is Off.

VT Display session

Host On-Demand's VT support is fully compliant with accepted standards and includes features unique to the product.

To configure a VT session, click **VT Display**, which brings up the window shown in Figure 7-25. Most of the fields in the various selections have identical requirements as on the 3270 and 5250 settings. Refer to "3270/5250 Connection selection" on page 280 for details. So only the differences will be discussed here in detail.



Connection

		Lock
Session Name	VT Display	□
Destination Address		☑
Destination Port	23	☑
Protocol	Telnet	☑
Screen Size	24x80	□
Host Code Page	DEC Multinational Replacement Character ...	☑
Inactivity Timeout (minutes)		□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 7-25 VT session Connection selection

VT Connection selection

The differences to a 3270 and 5250 session are:

- Destination Port

  Host On-Demand Version 8 introduces SSH as a additional secure protocol. The default port for a SSH session is 22.

- Protocol

  You can choose between Telnet, Telnet - TLS, Telnet - SSL only and SSH, which is new in Host On-Demand Version 8.

- Screen Size

  This parameter has many available screen sizes to choose from. You will probably find that most of them are very difficult to read; therefore, we recommend you use the 24x80 screen size unless your application requires a different size.

File transfer for VT host systems is performed with sftp; therefore, refer to “FTP/sftp session” on page 322 for details on how to configure the file transfer defaults.

VT Secure Shell (SSH) selection

If SSH has been selected as the protocol in the connection selection, the fields on the SSH selection shown in Figure 7-26 are enabled.

> **Note:** SSH is only available for VT sessions and Java 2 clients. JCE (Java Cryptography Extension) needs to be installed at the client. JCE is included in Java 1.4, if you are using Java 1.3, the JCE needs to be installed manually.

For a basic description of SSH please see 11.5, "Host On-Demand SSH support" on page 433

The fields on this selection panel are:

- User ID

  The user ID to be used for this SSH session. This ID is used both for Public Key Authentication and Password Authentication. The default is no user ID. If no user ID is specified then Host On-Demand will prompt the user for a user ID before starting the session.

  For a VT Display session the User ID and Password fields are on the SSH configuration window.

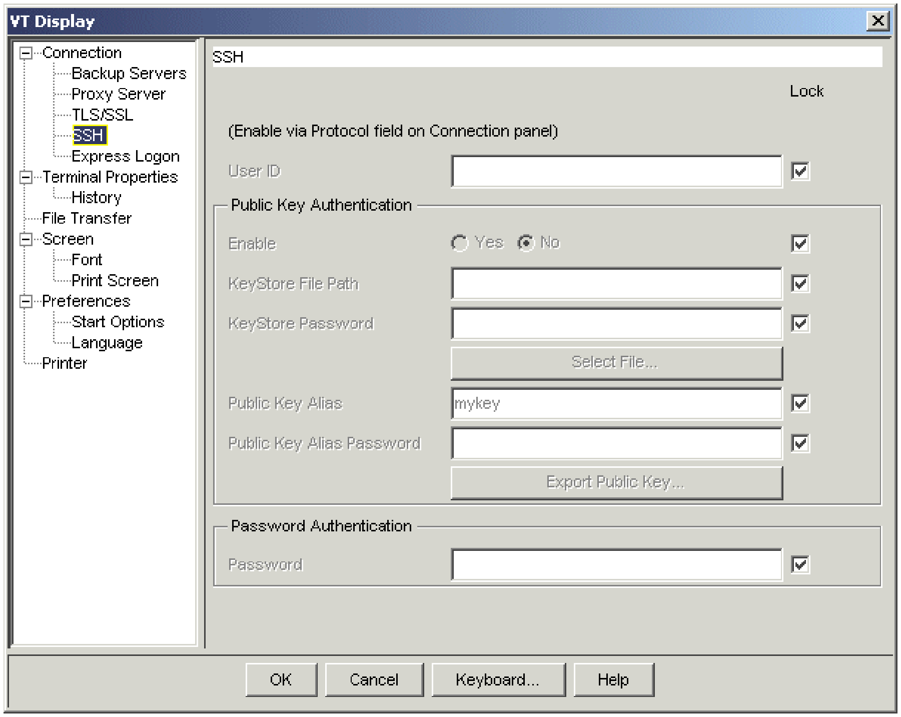
  For a FTP/sftp session the User ID and Password fields are on the Logon configuration window.

- Enable

  Enables public key authentication. Notice that, in contrast to public key authentication, password authentication is always enabled. The reason is that password authentication is used when public key authentication fails or when public key authentication is not enabled.

- KeyStore File Path

  The path and name of the keystore file on the client workstation containing the client's public and private keys. The default is no path or name. If no path or name is specified then Host On-Demand will search for the file keystore in the path specified in the Java system property user.home.



SSH

Lock

(Enable via Protocol field on Connection panel)

User ID ☑

Public Key Authentication

Enable ○ Yes ● No ☑

KeyStore File Path ☑

KeyStore Password ☑

Public Key Alias mykey ☑

Public Key Alias Password ☑

Password Authentication

Password ☑

Figure 7-26 VT session SSH selection

- KeyStore File Password

  The password required to open the keystore file on the client workstation. The default is no password. If no password is specified then Host On-Demand will prompt the user for a password before starting the session.

- Select File

  Opens a dialog that allows you to browse for the keystore file to be used.

- Public Key Alias

  Alias for the public-private key pair to be used in this session. A keyword alias is a descriptive string used to identify the key. The default alias is mykey.

- Public Key Alias Password

  The password required to read the public key information from the keystore. If no password is specified then Host On-Demand will attempt to read the public key information using a null password (no password). If the attempt to read the public key information using a null password fails then Host On-Demand will attempt to read the public key information using the same password as is specified in the KeyStore Password field above. If the attempt to read the public key information using the KeyStore Password fails then Host On-Demand will prompt the user for the password.

- Export Public Key

  Launches the Export Public Key utility. See Export public key in the help for a detailed description.

- Password

  The password to be used for password authentication for the client. The default is no password. If no password is specified then Host On-Demand will prompt the user for the password before starting the session. For a VT Display session the User ID and Password fields are on the SSH configuration window.

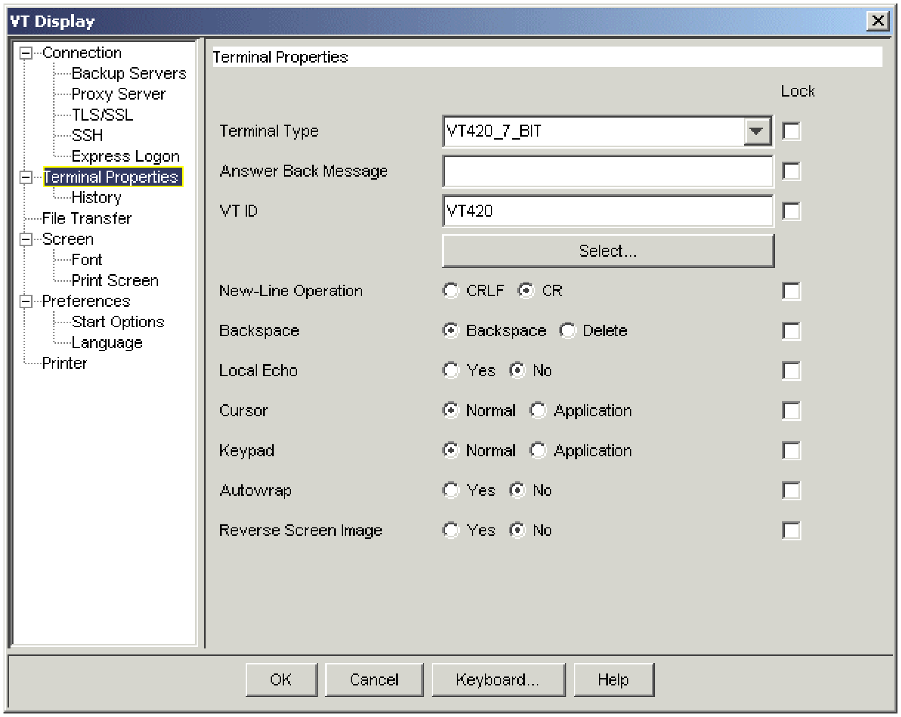
  For an FTP/sftp session the User ID and Password fields are on the Logon configuration window.

For more information about SSH refer to 11.5, “Host On-Demand SSH support” on page 433.

Note: At the time the book was published, there was a open problem in Java causing a SSH session to fail at startup when using a download client. The workaround was to use the cached client instead.

VT Terminal Properties selection

VT displays have characteristics that are different from 3270 and 5250 sessions. See Figure 7-27.



Terminal Properties

		Lock
Terminal Type	VT420_7_BIT	□
Answer Back Message		□
VT ID	VT420	□
New-Line Operation	○ CRLF ● CR	□
Backspace	● Backspace ○ Delete	□
Local Echo	○ Yes ● No	□
Cursor	● Normal ○ Application	□
Keypad	● Normal ○ Application	□
Autowrap	○ Yes ● No	□
Reverse Screen Image	○ Yes ● No	□

Figure 7-27 VT Terminal Properties selection

- Terminal Type

  Defines the type of VT emulation you want to use, which depends on the types supported by your host system. The types listed in the drop-down menu are:

  – VT420 7-bit (default)
  – VT420 8-bit
  – VT100
  – VT52

  > **Note:** If you require VT220 or VT320, specify VT420, which supports VT220 mode.

  For VT emulation limitations, see the online help for the display tab by clicking the **Help** button in the VT session display tab window.

- Answer Back Message

The Answer Back Message is used to return a message to the host when the host inquiry command is sent to the terminal. Enter into this field anything that you wish returned in response to a `query` command.

- VT ID

  Virtual Terminal ID. The virtual terminal id is a character string used to identify the type of terminal to be emulated. The default value is VT420. To enter a different value use one of the following methods:

  - Basic method. Click **Select**... When the VT ID popup appears, click the value you want. Then click Apply to add the value to the VT ID field or click Cancel to cancel.
  - Advanced method. Do not click Select. Type the value you want directly into the VT ID field. For example, you might type vt100. Use this method if the value you want is not available through the basic method.

- New-Line Operation

  Specifies where the cursor will move when you press the **New Line** key. The default is CR.

  - Click **CRLF** if the cursor must move to the left margin on the next line.
  - Click **CR** if the cursor must move to the left margin on the same line.

- Backspace

  Defines the default behavior of the backspace key; however, the actual action of the key is determined by the host application. The default is Backspace.

  - Click **Backspace** to send a standard ASCII backspace control-code (x'7F'). This moves the cursor backwards one position.
  - Choose **Delete** to send a standard ASCII delete control-code (x'08'). This moves the cursor back one position and deletes the character in that position.

- Local Echo

  Specifies where characters are sent when you type them.

  - Click **Yes** to send characters to the host and to the display. Depending on how the host system behaves, you might get double characters on the screen.
  - Click **No** to send characters to the host and depend on the host to send them back to the display.

  The default is No, which means that characters will display only once.

- Cursor

  Click **Normal** to use the arrow keys to move the cursor to different positions on the screen.

Click **Application** to use the cursor keys to send control-code sequences that can be read by host applications. To determine whether the Application option is required, refer to the application's documentation.

- Keypad

  Click **Normal** to use the VT auxiliary keypad for typing numbers.

  Click **Application** to use the VT keypad buttons to send control-code sequences that can be read by host applications. To determine whether the Application option is required, refer to the application's documentation.

- Autowrap

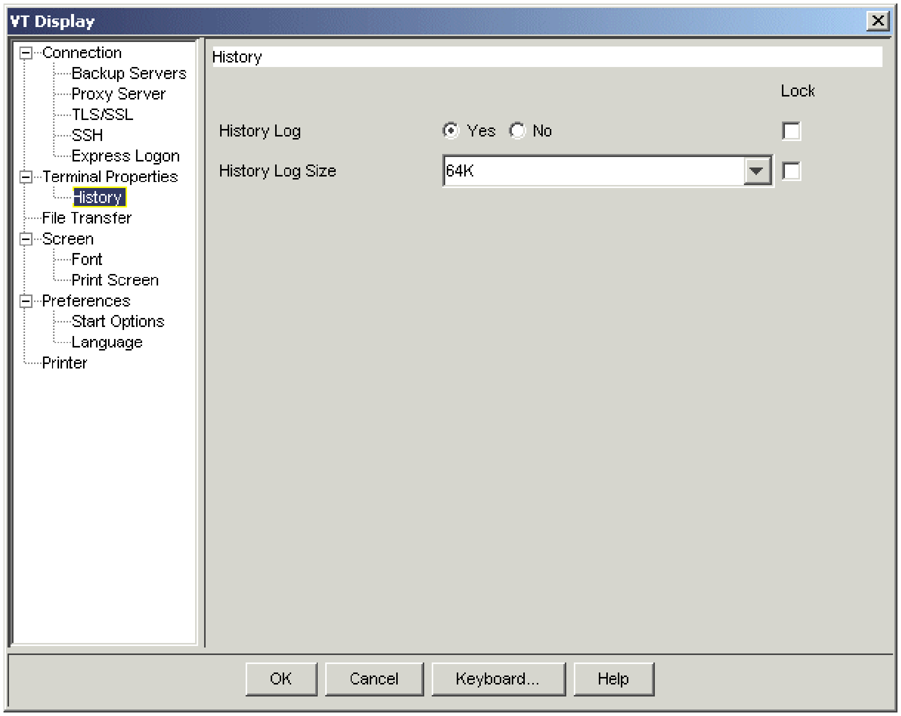
  Specifies whether the text must automatically continue to a new line when it reaches the margin on the current line.

- Reverse Screen Image

  Reverses the foreground and background colors.

VT History selection

- This selection does not appear in a 3270/5250 display session configuration.



History

Lock

History Log ● Yes ○ No □

History Log Size 64K □

Figure 7-28 VT History selection

- History log

  The Host On-Demand history log can be turned on or off by clicking the **History Log** radio button; the size is controlled by a drop-down menu.

- History Log Size

  The administrator can set the log size at increments between 16 KB and 512 KB. Once a VT session is configured to use the history log feature, the user will have access to the history log, which is highlighted in reverse video. You cannot use Host On-Demand's Copy function to get more than one screen's worth of data to the clipboard. By scrolling back and using the Copy Append function, it is possible to get as much of the history log as desired onto the clipboard before pasting it into another application. We found that the default of 64 KB for History Log Size was sufficient.

VT Preferences selection

There is one parameter in addition to the ones already explained at the 3270/5250 display session Preferences selection.

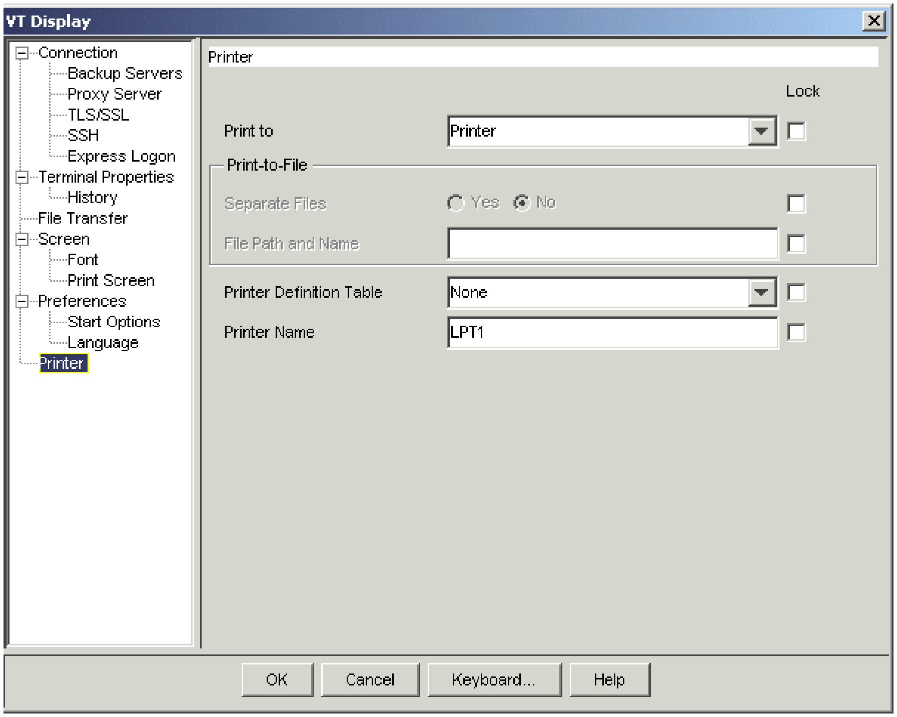
- Move Cursor On Mouse Click

  Specifies whether the cursor should move when you click the mouse on the screen.

VT File Transfer selection

File transfer for VT host systems is performed with FTP; therefore, refer to "FTP/sftp session" on page 322 for details on how to configure the file transfer defaults.

VT Printer selection



Printer

Lock

Print to: Printer □

Print-to-File

Separate Files ○ Yes ● No □

File Path and Name: □

Printer Definition Table: None □

Printer Name: LPT1 □

Figure 7-29 VT printer selection

- Print To

  Select to print to a local Windows printer (Windows platforms only), to another type of printer (for example, LPT1), or to a file. On Windows platforms, the default is Windows Printer. On non-Windows platforms, the default is Printer. On Mac OS X, the default is File.

- Print-to-File

  This group box lists the options that are used for printing to a file instead of a printer.

  – Separate Files

    When the print destination is a file, you can choose whether you want to save each print job to a unique file or to have jobs appended to each other in one file. When the Use Adobe PDF option is set to Yes, this option is not available and each print job is saved to a unique file. See help for more information.

  – File Path and Name

When the print destination is a file, type the path and name of the file. If the file path and name already exist on the client, Host On-Demand will print the file to that destination and will overwrite any files that already exist there. If the file path and name do not exist on the client, they are automatically created and the files will be printed to that destination. You can then view or print the file using the appropriate viewer on the client.

Note: If you do not type the path of the file, Host On-Demand will write the file to your browser's default directory. Your browser's default directory depends on your operating system. Refer to the Host Printing Reference for more information.

- Printer Definition Table

  A printer definition table (PDT) formats print data sent by the host application so it can be printed on a workstation printer. The PDT you select must be suitable for the printer and for the printer-emulation mode that the printer will use (PCL, PPDS, and so on; note that PostScript is not supported). You can create your own PDTs, which are automatically added to the pull-down list.Select a name from the pull-down list.If you are not sure which printer emulation modes are supported by your printer, you must refer to the printer's technical documentation, which usually lists the supported modes. See the online help for additional information.

- Printer Name

  Type the name of the port for the printer you want to use. On Windows workstations, you can also type the UNC (Universal Naming Convention) name of a network printer in either of two formats:

  – \\server_name\printer name

  – \\server's_host_name_or_IP_address\printer name

  For example, if you are configuring a printer on Windows 95 or NT, you can type a port name such as LPT1, or a network printer name such as \\myhost\printer. If you are configuring a printer on UNIX, type a device name such as /dev/lp0.

- Lock

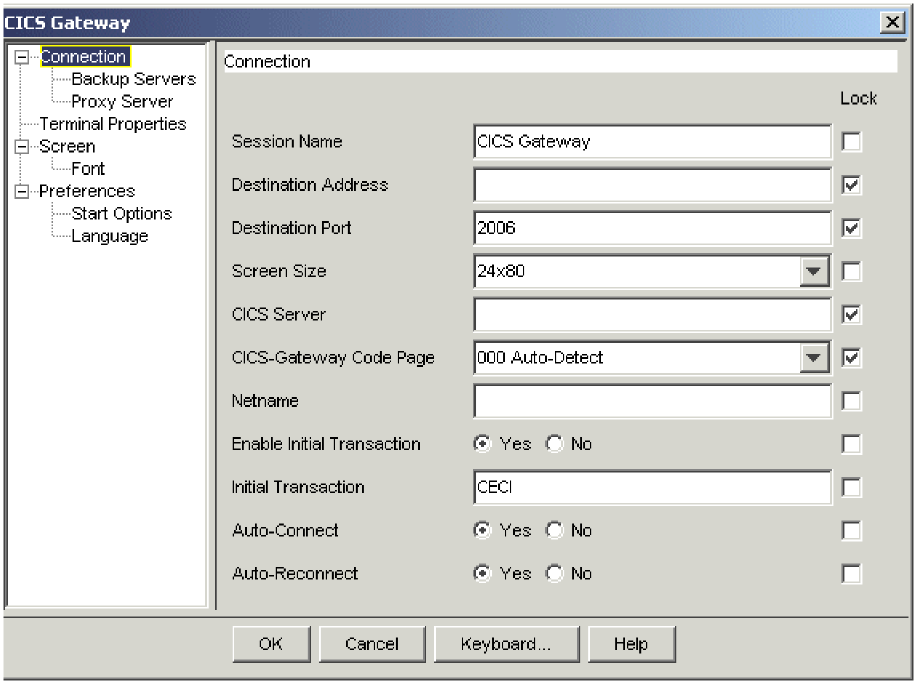
  Select Lock to prevent users from changing the associated startup value for a session. You cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

CICS Gateway client

The CICS Gateway client is a special session that communicates only to the CICS Transaction Gateway. It has limited functionality; for example, it does not support SSL sessions. A more functional choice would be to use the 3270 emulator client.

In order to use CICS Gateway client, you will need CICS Transaction Gateway Server V5.0.1 or later.

To configure a VT session, click **CICS Gateway**, which brings up the window shown in Figure 7-30.



		Lock
Session Name	CICS Gateway	☐
Destination Address		☑
Destination Port	2006	☑
Screen Size	24x80	☐
CICS Server		☑
CICS-Gateway Code Page	000 Auto-Detect	☑
Netname		☐
Enable Initial Transaction	● Yes ○ No	☐
Initial Transaction	CECI	☐
Auto-Connect	● Yes ○ No	☐
Auto-Reconnect	● Yes ○ No	☐

Figure 7-30 CICS gateway Connection selection

CICS Connection® selection

The CICS Gateway client requires some unique configuration parameters:

- CICS Server

  Specify the name of the CICS server to which the session connects. If this field is blank, the CICS Transaction Gateway's default server is used.

- CICS-Gateway Code-Page

  Specify the code page in use by the operating system at the CICS Transaction Gateway. If this field is set to `000 Auto-detect`, Host On-Demand normally retrieves the code page setting from the CICS Transaction Gateway; if that is not possible, you must get the correct code page from the network administrator.

- Netname

  The name of the terminal resource to be installed or reserved. If this field is blank, the selected terminal type is not predictable.

  This option is available for CICS sessions only.

- Enable Initial Transaction

  Select Yes to begin your session with an initial transaction. If you select No, the CICS session starts without a transaction: when you connect with the host, your session screen is blank. (Selecting No deactivates the next field, Initial Transaction.) The default is Yes.

- Initial Transaction

  The name of the CICS transaction that begins with the start of your session. This field is pre-filled with CECI, over which you may type the name of a different transaction.

- Auto-Connect

  Automatically connects the session to the target Telnet server. If you set this to No, you must click Connect in the session menu every time you want to connect a session. The default is Yes.

- Auto-Reconnect

  Reconnects the session automatically if communications fails and later recovers. The default is Yes.

- Lock option

  Select **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

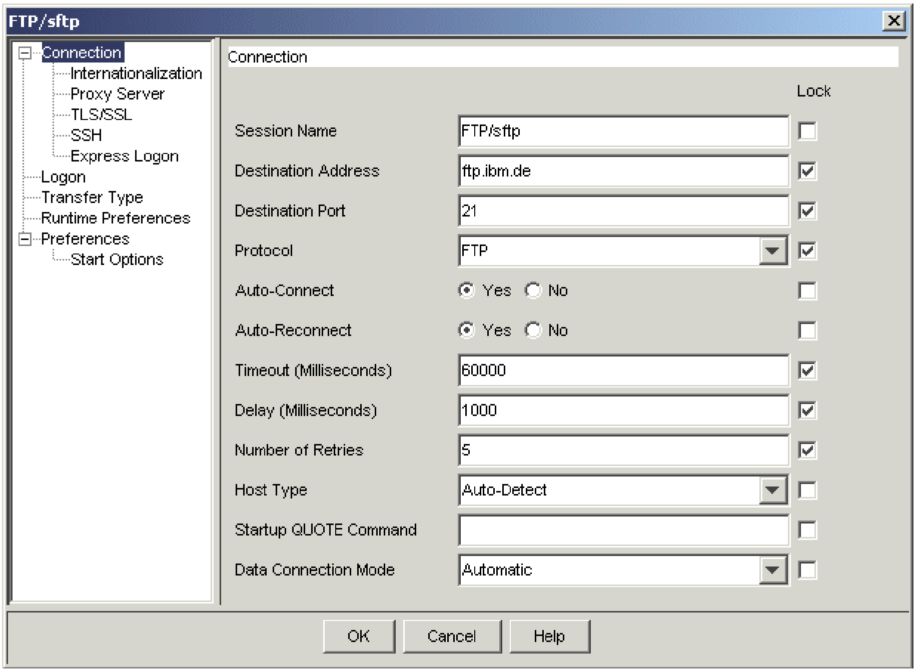
All other selection fields have identical requirements as on the 3270 and 5250 display session settings. Refer to “3270 and 5250 Display Sessions” on page 279 for details.

FTP/sftp session

The FTP/sftp session lets you copy files and directories from or to another system that supports FTP or sftp. The functions of the FTP session have been enhanced to provide secure file transfers and allow the use of proxys. The panels are almost equal to the ones at the 3270 display session.

FTP/sftp connection selection

This selection, shown in Figure 7-31, specifies all connection information for both sessions.



Connection

		Lock
Session Name	FTP/sftp	□
Destination Address	ftp.ibm.de	☑
Destination Port	21	☑
Protocol	FTP	☑
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□
Timeout (Milliseconds)	60000	☑
Delay (Milliseconds)	1000	☑
Number of Retries	5	☑
Host Type	Auto-Detect	□
Startup QUOTE Command		□
Data Connection Mode	Automatic	□

Figure 7-31 FTP session Connection selection

Use the following information to complete this window:

- Session Name, Destination Address, Destination Port, Protocol, Auto-Connect, Auto-Reconnect

  These parameters are the same as those for 3270/5250 sessions, so refer to “3270 and 5250 Display Sessions” on page 279.

  The default port is 21 for FTP, the default port for sftp is 22.

  Please refer also to 11.5.6, “sftp” on page 443.

- Timeout (milliseconds)

Sets the FTP/sftp connection timeout in milliseconds. To prevent the connection from ever timing out set this value to 0. The default is 60000.

- Delay (milliseconds)

  Sets the delay, in milliseconds, between connection retry attempts. Auto-reconnect must be set to `Yes`. The default is 1000.

- Number of Retries

  Sets the maximum number of connection attempts. A value of 0 will cause the session to try connect to the FTP server until a connection is made, or you cancel the attempt. Auto-reconnect must be set to `Yes`. The default is 5.

- Host Type

  Defines the FTP server's directory/file format style. Valid values are Auto-Detect, MS-DOS, MVS, Novell, OpenVMS, OS/2, OS/400, OS/400-UNIX, UNIX, and VM. The default is Auto-Detect. You should only change this value if you are having trouble seeing the remote system's file list (for example, when the remote file list panel displays only file folders and no other data, or the format of the data is incorrect). For more information see the online Help.

- Startup QUOTE Command

  Sends an uninterpreted string of data to the FTP server as the session starts. The Startup Quote Command allows you to set FTP server supported options when starting the session. For example, to set the host translation table, type `site trans [translation table name]` in the dialog box.

- Data Connection Mode

  - Active (PORT)

    The FTP client always uses active/normal mode for data connection.

  - Automatic

    If you select **Automatic** with an IPv6 FTP client or server, the FTP client attempts an Extended Passive (EPSV) transfer.

    If you select Automatic with an IPv4 FTP client or server and a secure connection, the FTP client attempts an Extended Passive (EPSV) transfer. If the Extended Passive transfer fails, the FTP client attempts active transfer (PORT). If active transfer fails, the FTP client attempts passive transfer (PASV).

    If you select Automatic with an IPv4 FTP client or server and a non-secure connection, the FTP client attempts active transfer (PORT). If active transfer fails, the FTP client attempts passive transfer (PASV).

  - Extended Passive (EPSV)

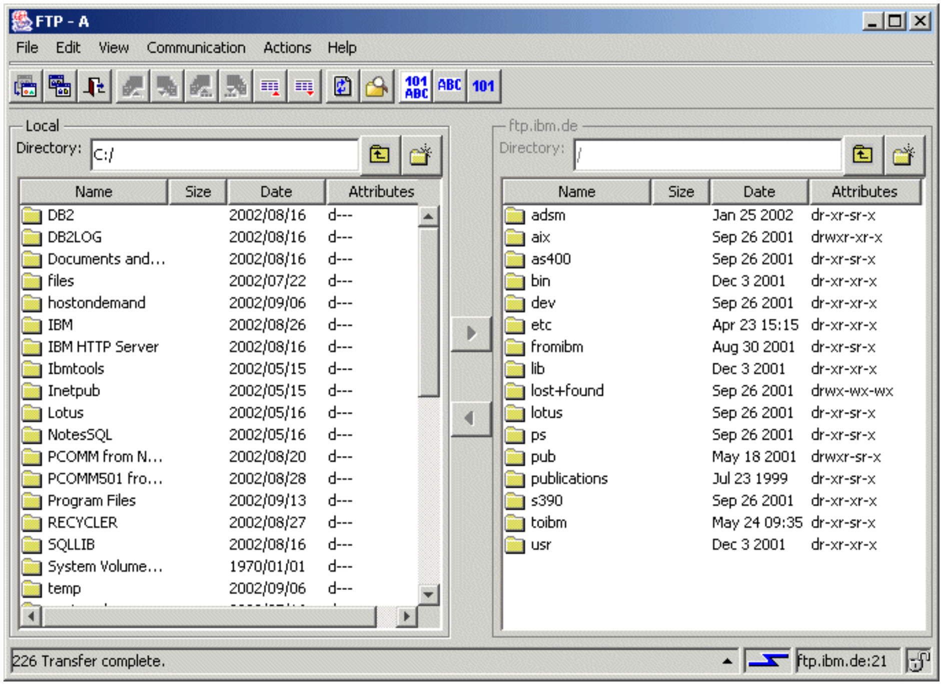
The FTP client uses Extended Passive for passive data connections to secure FTP servers that support this command or IPv6 FTP servers.

– Passive (PASV)

The FTP client always uses passive mode for data connection.

The default is Automatic. For additional information see Help.

Figure 7-32 shows the example of an established FTP/sftp session using the settings as filled in according to Figure 7-31.



Local

Directory: C:/

Name	Size	Date	Attributes
DB2		2002/08/16	d---
DB2LOG		2002/08/16	d---
Documents and...		2002/08/16	d---
files		2002/07/22	d---
hostondemand		2002/09/06	d---
IBM		2002/08/26	d---
IBM HTTP Server		2002/08/16	d---
Ibmtools		2002/05/15	d---
Inetpub		2002/05/15	d---
Lotus		2002/05/16	d---
NotesSQL		2002/05/16	d---
PCOMM from N...		2002/08/20	d---
PCOMM501 fro...		2002/08/28	d---
Program Files		2002/09/13	d---
RECYCLER		2002/08/27	d---
SQLLIB		2002/08/16	d---
System Volume...		1970/01/01	d---
temp		2002/09/06	d---

ftp.ibm.de

Directory: /

Name	Size	Date	Attributes
adsm		Jan 25 2002	dr-xr-sr-x
aix		Sep 26 2001	drwxr-xr-x
as400		Sep 26 2001	dr-xr-sr-x
bin		Dec 3 2001	dr-xr-xr-x
dev		Sep 26 2001	dr-xr-xr-x
etc		Apr 23 15:15	dr-xr-xr-x
fromibm		Aug 30 2001	dr-xr-sr-x
lib		Dec 3 2001	dr-xr-xr-x
lost+found		Sep 26 2001	drwx-wx-wx
lotus		Sep 26 2001	dr-xr-sr-x
ps		Sep 26 2001	dr-xr-sr-x
pub		May 18 2001	drwxr-sr-x
publications		Jul 23 1999	dr-xr-sr-x
s390		Sep 26 2001	dr-xr-xr-x
toibm		May 24 09:35	dr-xr-sr-x
usr		Dec 3 2001	dr-xr-xr-x

226 Transfer complete.

ftp.ibm.de:21

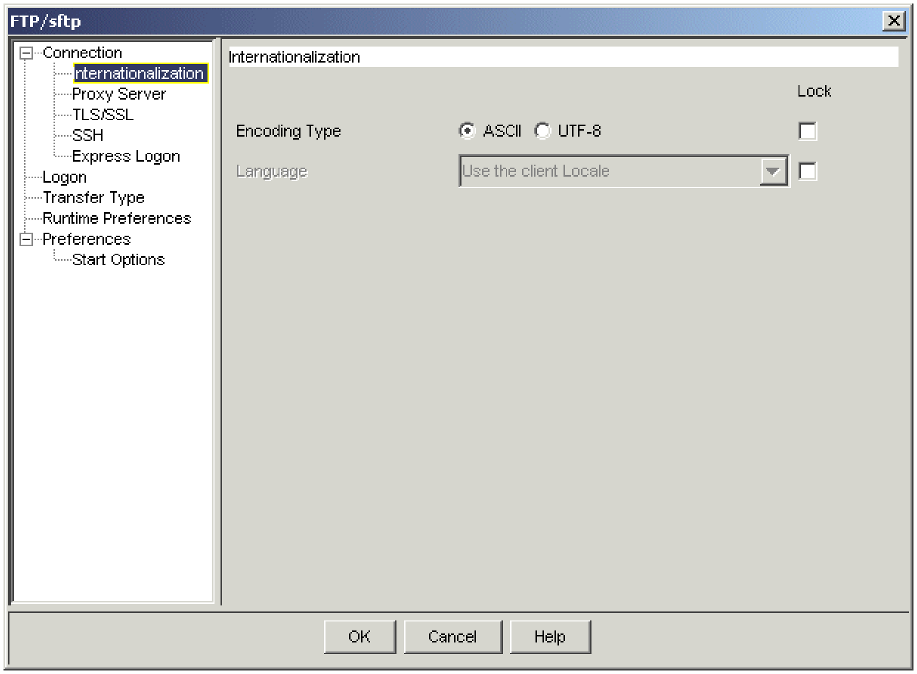
Figure 7-32 Example of established FTP connection

Note: If you experience problems with secure FTP sessions, and you are using a firewall, please check IETF Internet-Draft FTP/TLS Friendly Firewalls at:

```
http://www.ietf.org/internet-drafts/draft-fordh-ftp-ssl-firewall-03.txt
```

FTP Internationalization selection

The FTP Internationalization selection allows you to specify the character encoding type to use for the FTP session, along with the language selection for UTF-8 encoding.



Internationalization

Lock

Encoding Type ● ASCII ○ UTF-8 □

Language Use the client Locale □

Figure 7-33 FTP Internationalization selection

- Encoding Type

  If you select **UTF-8**, the FTP client converts file names and path names to UTF-8 before sending them to the server, and converts the file names and path names to the local client encoding when receiving the files from the server. For this to happen, the FTP server must support UTF-8 encoded path names. The default is ASCII when there is no conversion.

- Language

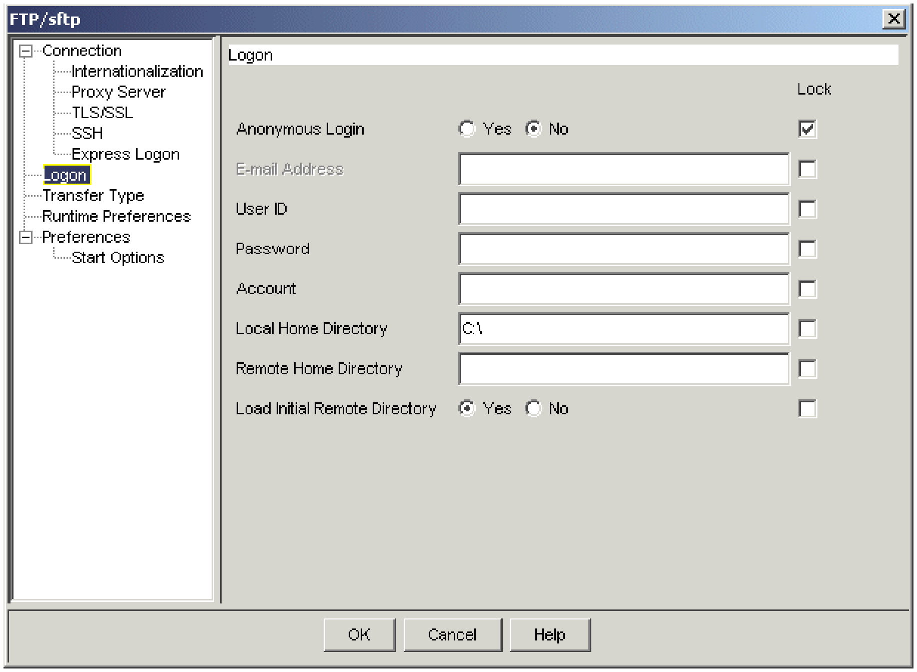
  Enabled if you select **UTF-8 encoding type**. Select a language for FTP greetings and error messages. The default is the language of the Host On-Demand client. If the FTP server does not support the language you select, or the default Host On-Demand client language, then the greetings and error messages appear in English.

- Lock (Host On-Demand administrator only)

  Check **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

FTP Logon selection

The Logon selection shown in Figure 7-34 contains the information required to gain access to the target system.



Logon

		Lock
Anonymous Login	○ Yes ● No	☑
E-mail Address		□
User ID		□
Password		□
Account		□
Local Home Directory	C:\	□
Remote Home Directory		□
Load Initial Remote Directory	● Yes ○ No	□

Figure 7-34 FTP Logon selection

- E-mail Address

  This field is enabled only when **Anonymous Login** is selected, and specifies the e-mail address to use as the password when connecting to the FTP server. If this field is blank, the session also sends `anonymous` as the password to the FTP server.

- User ID

  Specifies the user ID the session uses when connecting to the FTP server. **Anonymous Login** must be disabled. If User ID is blank, you will be prompted for a user ID and password when the session attempts to connect to the FTP server.

- Password

Specifies the password the session uses when connecting to the FTP server. If **Password** is blank, you are prompted for a password when the session connects to the FTP server. The password is not encrypted when it is sent to the FTP server. If Anonymous Login is set to `Yes` then the e-mail address is sent to the FTP server as the password. If E-mail Address is blank and Anonymous Login is set to `Yes`, anonymous is also sent to the FTP server as the password.

- Account

  Specifies the FTP server account name the session uses when connecting to the FTP server. Not all FTP servers use accounts. Check with the FTP server administrator if you need an account.

- Local Home Directory

  Sets the initial directory on your PC when the session connects to the FTP server. After the session connects, you can change the directory by entering a valid directory in the Directory field by clicking the directory button next to the Working Directory field, and by double-clicking a directory folder in the local file list.

  The default is c:\.

- Remote Home Directory

  Sets the initial directory on the FTP when the session connects to the FTP server. After the session connects, you can change directory by entering a valid directory in the Directory field, by clicking the directory button next to the Working Directory field and by double-clicking a directory folder in the remote file list.

  The default is the initial login directory set by the FTP server at login. If you enter a valid directory in this field, it will over-ride the login directory set by the server.

- Load Initial Remote Directory

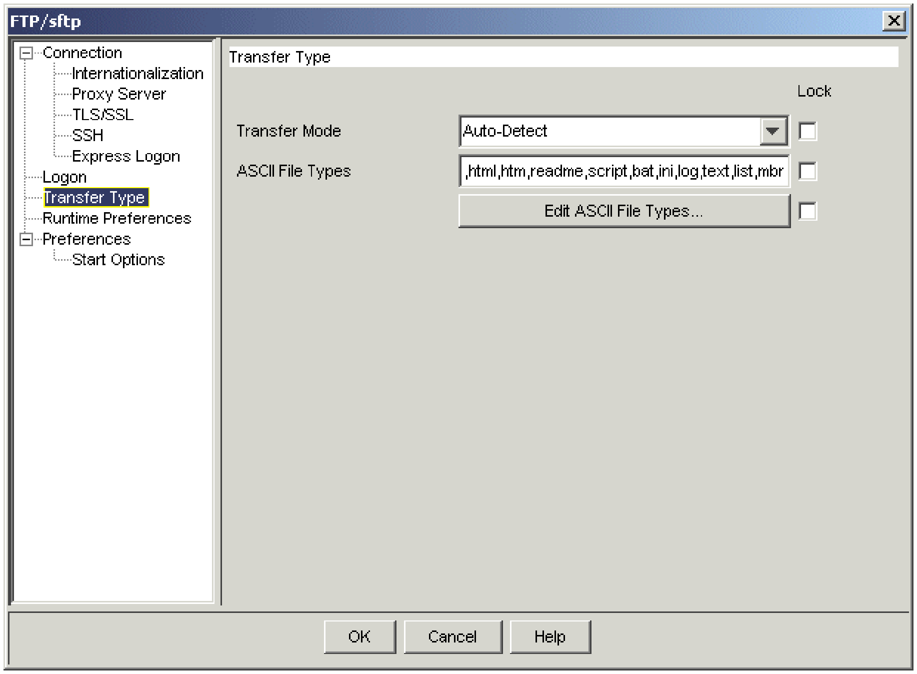
  In some FTP sites a subdirectory is so large that it might take a considerable amount of time until the FTP session can display it. To avoid the initial display of such subdirectories, select **No**. If you select **No**, the user must do one of the following for the host directory listing to appear:

  - Type a path in the Directory field.
  - Refresh the remote listing.
  - Upload a file or directory.

  The default is Yes, which shows the content of the remote subdirectory at session connect.

FTP Transfer Type selection

This selection shown in Figure 7-35 describes how the data in the files to be transferred should be treated.



Transfer Mode: Auto-Detect □

ASCII File Types: ,html,htm,readme,script,bat,ini,log,text,list,mbr □

Figure 7-35 FTP Transfer Type selection

- Transfer Mode

  Sets the default file transfer mode. Valid values include ASCII mode, Binary mode and Auto-detect. ASCII files are typically plain text files, while binary files can execute graphics or a proprietary format (for example, database .dbf and MS Word .doc files). Auto-detect automatically selects the proper file transfer mode for each file based on the file's extension. Files with an extension listed in the ASCII File Types list are transferred as ASCII files. Files with an extension not listed in the ASCII File Types list are transferred as binary files. The default is Auto-detect.

- ASCII File Types

  Determines which files are transferred in ASCII mode instead of binary mode when Default Transfer Mode is set to Auto-detect. Files with an extension listed in this list are transferred as ASCII files. Files with an extension not listed in this list are transferred as binary files

- Edit ASCII File Types

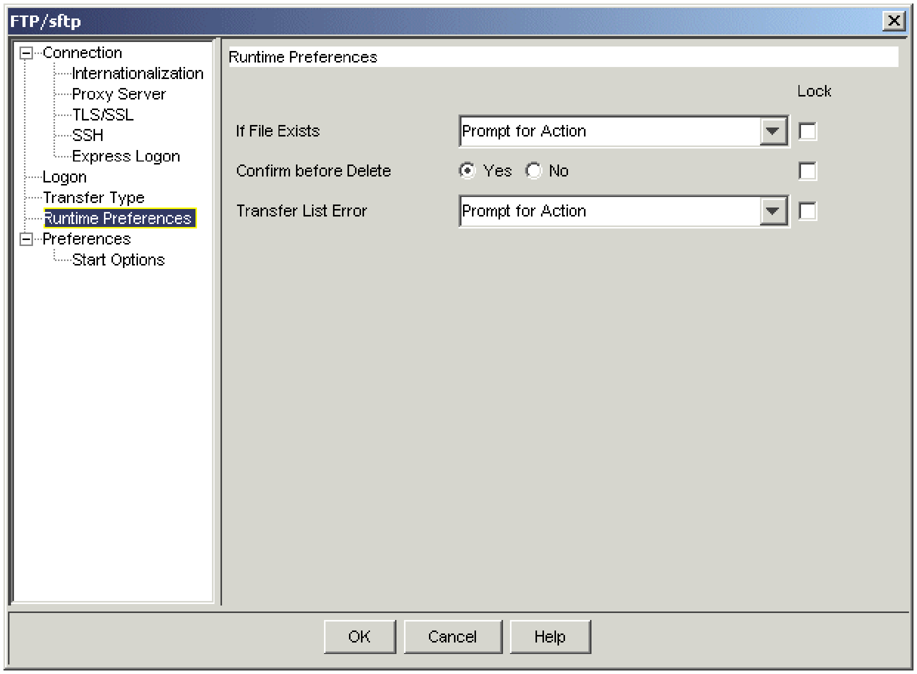
Allows you to add and remove entries in the list of ASCII File Types. To add an ASCII File Type, click the **Edit ASCII File Types** button. Enter the text to associate with the ASCII mode in the dialog box that displays, and then click **Add**. To add multiple entries, type each one into the dialog box, separated by commas (**,**) and click **Add**. To remove an ASCII File Type, click the **Edit ASCII File Types** button. Select the **File Type** from the list in the dialog box, and click **Remove**. To remove multiple entries, select entries by selecting them and clicking **Remove**. Click **OK** when you are finished editing ASCII File Types.

- Lock (Host On-Demand administrator only)

  Check **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

FTP Runtime Preferences selection

This selection shown in Figure 7-36 allows you to determine the default actions taken by the FTP client during a file transfer.



Runtime Preferences

Lock

If File Exists: Prompt for Action □

Confirm before Delete: ● Yes ○ No □

Transfer List Error: Prompt for Action □

Figure 7-36   FTP Runtime Preferences

- If file exists

  Determines what action the session takes if the file already exits. Choices include Overwrite Existing, Prompt for Action, and Skip the File. When set to Prompt for Action, you can choose to Overwrite, Save As, Skip the File, or Cancel. The default is Prompt for Action.

- Confirm before Delete

  Prompts for confirmation before a file is deleted. The default is Yes.

- Transfer List Error

  Allows you to choose what happens if an error occurs during the upload or download of a transfer list. If you select **Prompt for Action**, a window appears allowing you to continue or cancel the transfer. If you select **Continue**, the transfer of the remaining files or directories in the list continues. When the transfer is complete, a window appears with the number of errors during the transfer. Click **Show Errors** to view the errors.

- Lock (Host On-Demand administrator only)

  Check **Lock** to prevent users from changing the associated startup value for a session. Users cannot change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

FTP Preferences selection

The Preferences selection for FTP sessions reflects operational characteristics of the session. The fields are very much the same as the ones for the 3270 and 5250 Display Sessions, so only the differences will be discussed:

- Layout View

  Determines which of two graphical views your FTP session has at startup. You can change the Layout View on the session menu under View. Both views list file name, size, date, and attributes. Valid values are:

  – Side by Side View

    Provides a view of the remote and local file systems in two separate window panels adjacent to each other, with the remote file system on the left, and the local file system on the right. When the FTP client window is resized, the file lists are automatically resized.

  – Stacked View

    Provides a view of the remote and local file systems in two separate panels on top of each other, with the local file system on top of the remote file system. When the FTP client window is resized, the file lists are automatically resized.

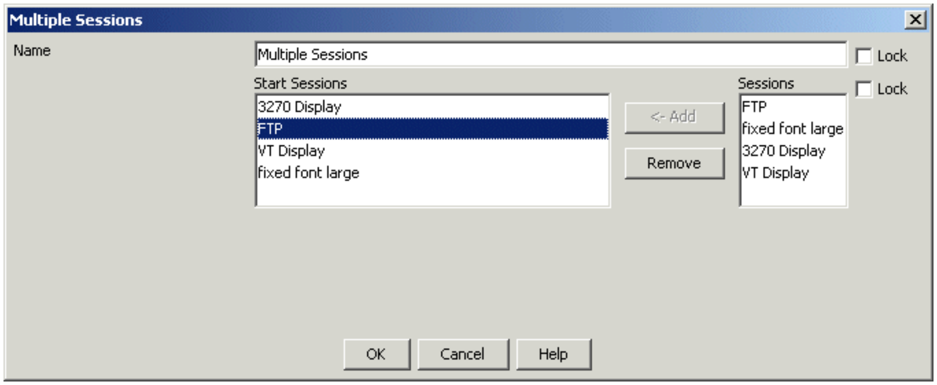
    The default view is Side by Side.

- Transfer List Manager

  Select **Yes** if you want the Transfer List Manager toolbar to be visible on the screen when the session starts. You can also display or hide the Transfer List Manager toolbar from the View menu. The Transfer List Manager allows you to create and transfer a list of files or directories. The default is No (not visible).

Multiple sessions

The multiple session object is a rather simple concept. A multiple session object is one that represents multiple Host On-Demand host sessions. When the user opens one of these objects, all of the sessions it represents are started. The configuration window is shown in Figure 7-37.



Name: Multiple Sessions □ Lock

Start Sessions: 3270 Display, FTP, VT Display, fixed font large

Sessions: FTP, fixed font large, 3270 Display, VT Display □ Lock

Figure 7-37 Multiple session configuration window

You must enter a unique name to identify the object. Next add sessions by highlighting a session from the right pane and clicking **Add**, repeating as necessary to place all desired sessions in the left pane. You may remove an unwanted session by selecting it from the left pane and clicking the **Delete** button. When completed you will have a session window similar to that shown in Figure 7-38.

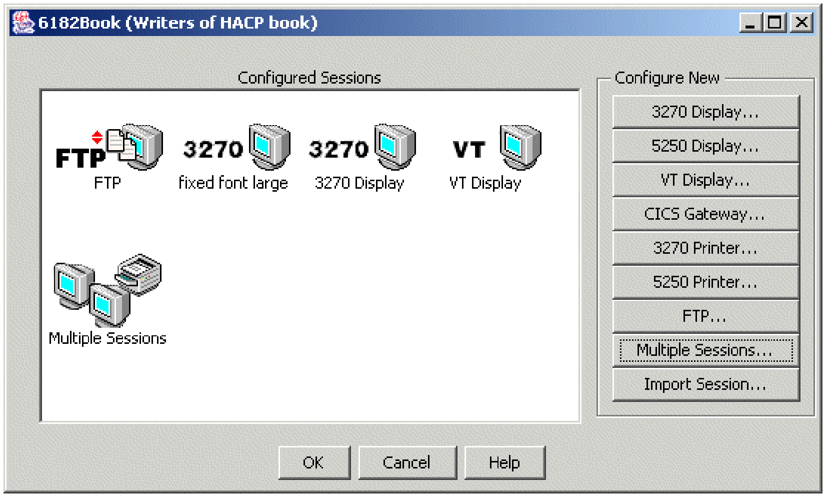


Figure 7-38 Configured Sessions window

When creating or modifying a multiple session object, keep in mind:

- To add more than one host session at a time, simply select additional sessions by using the Shift or Ctrl keys on the keyboard when selecting a host session. Then, when the desired sessions are selected, click the **Add** button.
- You can add the same session multiple times. When the object is opened, each of the sessions will open. So, if you add the same host session twice, two emulator sessions to that host will open when the user opens the multiple session object.

Multiple session object behavior

This section is a summary of what to expect when using the multiple session object:

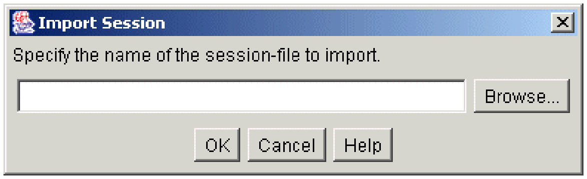
- A multiple session object can contain any Host On-Demand session object except another multiple session object.
- To add a Host On-Demand session to a multiple session object, the session must have been previously defined for that group or user.
- Launching a multiple session object will open all the sessions contained within.
- If a multiple session object is deleted, it does not delete the session objects it contains.
- If an administrator deletes a host session object that is contained within a multiple session object, a warning is displayed, but the pointer to the object is not removed. The administrator must delete it separately.

- Multiple session objects can be exported and imported. However, when such an object is exported, it does not export the host session objects that are contained within. Those must be exported and imported separately.

Import Sessions

The Import Sessions window is used to import exported Host On-Demand (.hod) sessions or sessions from Personal Communications (.ws).

Click **Import Session** to bring up the window shown in Figure 7-39.



Import Session

Specify the name of the session-file to import.

Figure 7-39 Import Session window

Simply type the name of the file or use the **Browse** button to locate the file on any file system accessible by the user. When you are finished, click **OK**.

You can import an existing session to create a new one. The existing session can be either a Telnet session from Personal Communications v4.1 or later, or a previously-exported Host On-Demand session.

If you are importing a session icon configured for multiple sessions, you must import all of the sessions contained within that configuration. For example, if the multiple session is configured to start a 3270 session, a 5250 session and a 3270 print session, then you need to import all three of those sessions along with the multiple session icon.

To import a session:

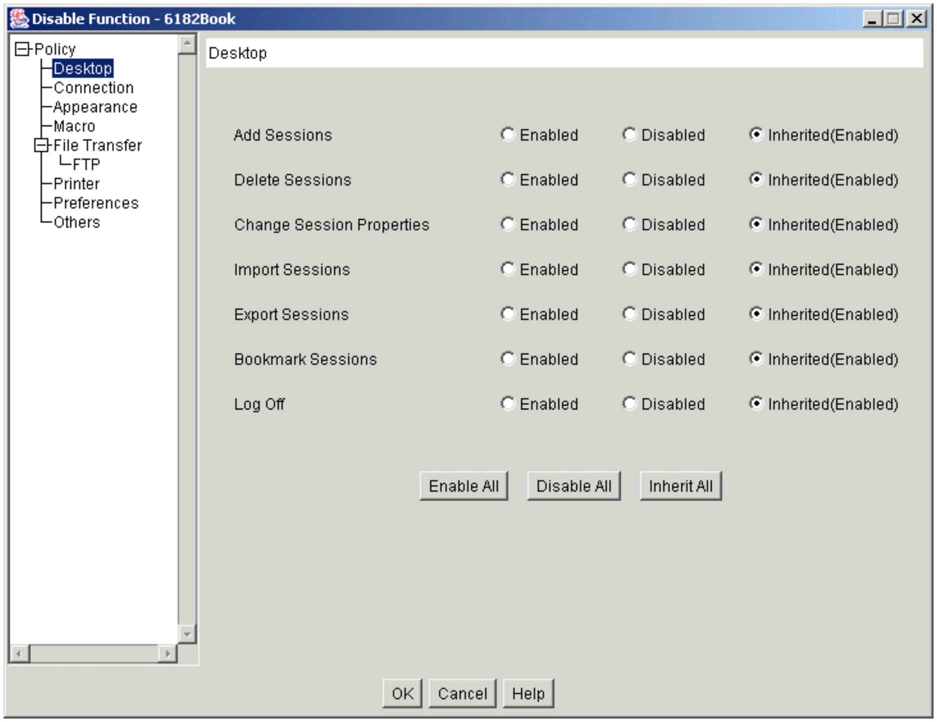
1. From the Client window, click **Add Sessions**, then **Import**.
2. Type the filename for the session you want to import, or click **Browse**. You can import:
   a. Session files previously created by exporting Host On-Demand sessions.
   b. Telnet sessions from Personal Communications v4.1 or later.
3. Click **OK**.
4. The session icon appears in the Configured Sessions area.

The sessions you import from other products (for example, Personal Communications) may not behave exactly as they did in the originating product. For example, for sessions imported from Personal Communications, Host On-Demand Version 8 will only map the settings in the .ws-file. The settings in the pcswin.ini file will not be mapped. There might also be a difference in the screen colors due to the fact that PCOMM and HOD use different RGB settings.

7.1.8 Disabling functions

When configuring users and groups, you can disable functions that you do not want users to access. You can disable any of the graphical interface items on pop-up menus and buttons in the Client window, the session menu, and the session toolbar. For example, you can remove items such as Copy, Export Session, or Properties from the pop-up menu in the client window or the macro button from the toolbar in the session window. When a function is disabled, it is removed from the toolbar or menus so users do not see it. Functions cannot be accessed using the shortcut keys either.

See Figure 7-40, which shows the disable functions for the desktop. Use the left pane to navigate to the available group of options, and select the behavior for the individual parameters on the right pane.



Desktop

Add Sessions	○ Enabled	○ Disabled	● Inherited(Enabled)
Delete Sessions	○ Enabled	○ Disabled	● Inherited(Enabled)
Change Session Properties	○ Enabled	○ Disabled	● Inherited(Enabled)
Import Sessions	○ Enabled	○ Disabled	● Inherited(Enabled)
Export Sessions	○ Enabled	○ Disabled	● Inherited(Enabled)
Bookmark Sessions	○ Enabled	○ Disabled	● Inherited(Enabled)
Log Off	○ Enabled	○ Disabled	● Inherited(Enabled)

Figure 7-40 Disable function

You cannot reduce download size by disabling functions. Disabling functions is different from locking functions. You can lock the fields of a function when you are configuring a session. Locking fields locks the startup values for a session. In most cases, users cannot change values for those fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

You can enable or disable functions for a group or user in either one of two ways:

- From the Administration window:
  a. Click **Users/Groups**.
  b. Right-click a group or user, and select **Disable Function**.
- From the Deployment Wizard:
  a. Define a host session.
  b. Click **Disable Functions**.

Changes made to a user’s functions while the user is logged on do not become effective until the user has logged off and then logs back on.

Inheriting from a group (Administration client only)

Enabling and disabling functions can be set for each group and for each user within a group. A user or group can be configured to use, or inherit, the settings for functions from a higher (parent) group. However, settings for functions at the lower level groups or users take precedence over the higher level groups. In other words, if you disable a function at a group level but enable it for a user in that group, the function is enabled for only that user. Because of the inheritance factor, it is easier to set functions at the group level, and then disable or enable specific functions for the users or groups belonging to those higher level groups.

If you are using an LDAP server for storing configuration information, a user can be a member of only one group. If you select **Inherit** for a function, whatever is set for that group is applied to the user.

If you are using the Host On-Demand configuration server local data store, a user can be a member of multiple groups. If you select **Inherit**, and all the groups to which the user is a member of have the function disabled, then the function is disabled for the user also. Or, the other way around: If one of the groups to which the user belongs has a function enabled, the user inherits this function and it is enabled.

See the online help for each group of options for a detailed description of the individual parameters. In general, you can select for each parameter:

- Enabled

  Allows group or user to access this function

- Enable All

  Enables all the functions listed on the current screen

- Disabled

  Does not allow groups or users to access this function

- Disable All

  Disables all the functions listed on the current screen.

- Inherited (Enabled) (Administration client only)

  Uses the setting to which this user or group is a member of. The inherited value is enabled.

- Inherited (Disabled) (Administration client only)

  Uses the setting to which this user or group is a member of. The inherited value is disabled.

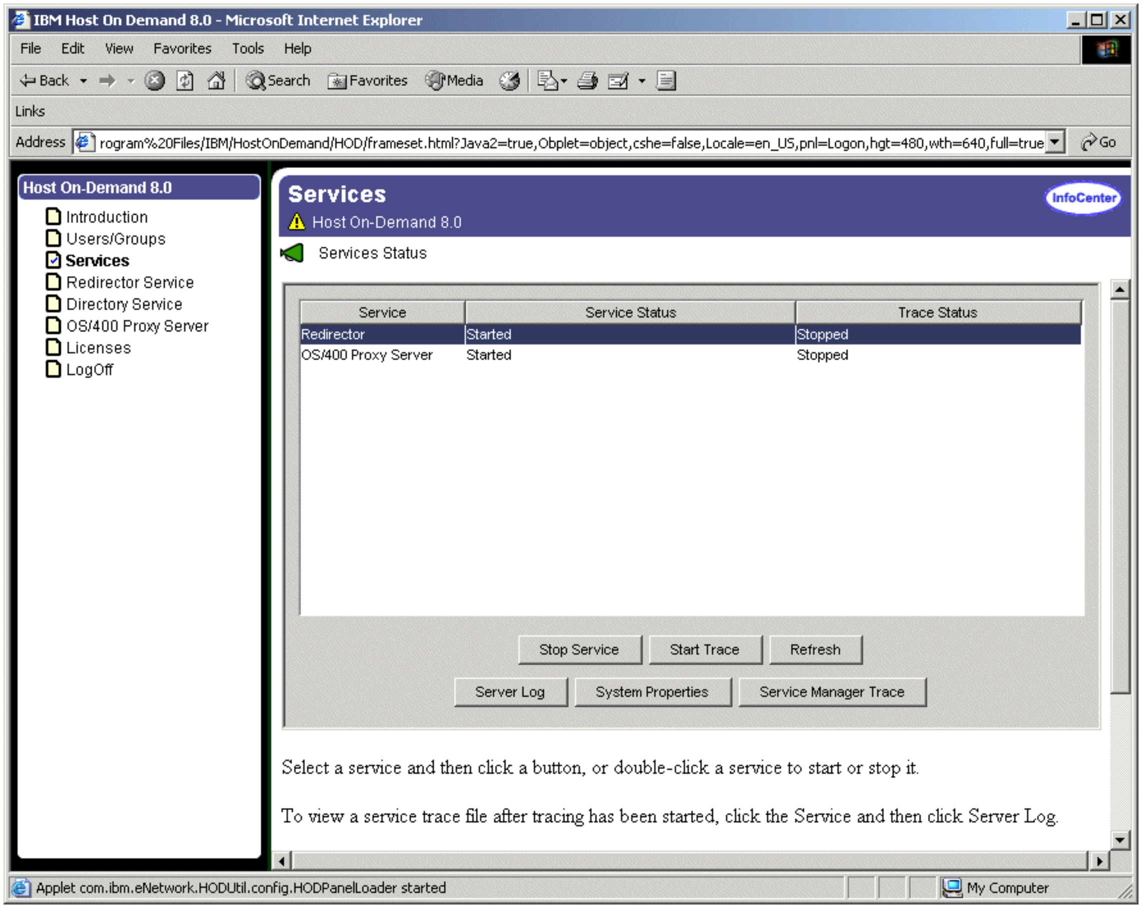
- Inherit All (Administration client only)

  Inherits all the functions listed on the current screen.

> **Note:** If a function that is disabled is represented by a pull-down menu and an icon on the toolbar, both are hidden from the user.

7.2 Services

The Services window in Figure 7-41 will be presented after you click the **Services** task in the Administration Notebook. Use the Host On-Demand Services window to manage Host On-Demand services. This window shows the status of each service, the status of the trace option for each service, and lets you view the server's message and trace log. You can also refresh the view to see the current status of each service.



rogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true

Service	Service Status	Trace Status
Redirector	Started	Stopped
OS/400 Proxy Server	Started	Stopped

Select a service and then click a button, or double-click a service to start or stop it.

To view a service trace file after tracing has been started, click the Service and then click Server Log.

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 7-41 Services administration window

The following services are available:

- The Redirector gives clients access to Telnet hosts other than the Web server from which they were downloaded. The Redirector supports TLS security. The Service status (started or stopped) and the trace status (started or stopped) remains the same across a Service Manager start or stop for the Redirector.
- The O/S400 Proxy Server enables all the data to flow through one configured port instead of multiple ports. The Service status (started or stopped) and the trace status (started or stopped) remains the same across a Service Manager start or stop for the OS/400 Proxy Server.
- Trace allows you to start and stop the server's trace facility, which lets you capture and view information that can help in resolving problems.
- Service Manager Trace allows you to stop, start, and set the trace level for the Service Manager's trace facility, which lets you capture and view information that can help in resolving problems with the Service Manager. The current service status and trace status remain the same across Service Manager stops and restarts.

Starting and stopping a service or trace

To start and stop a service or trace, here are the steps:

1. Highlight the service.
2. Click the **Start/Stop Service** or **Start/Stop Trace** button (depending on which service you are starting or stopping). The Start service and Start trace buttons alternate between start and stop. For example, if you click the **Start Service** button to begin a service, this same button automatically changes to Stop Service.
3. To see message or trace information created by the Redirector, click **Server Log**. To make the log easier to read, copy the information to the clipboard and paste it into a file.

Tracing the Service Manager:

1. Click **Service Manager Trace** to display the Service Manager Trace window.
   - Trace Active

     To turn tracing on, click **Yes**. To turn tracing off, click **No**.
   - Trace Level

     Set the Trace Level by selecting a value from **1** (collects only critical messages) to **3** (collects detailed trace information).
2. Click **Apply** to start the service manager trace. The trace status and trace level remain the same across Service Manager starts and stops.

The trace is saved in the \private subdirectory as NCoDServices.RAS.txt. The trace settings are saved in \private subdirectory as NSMprop.

7.3 Redirector service

The Redirector is a Telnet proxy that is able to accept connections from clients and pass them on through a different port to the next stage in the link. The Redirector can serve as a barrier between clients and the target Telnet server. If you do not want a large number of clients connecting directly to your host system because of a security risk, you can have the clients connect to one or more Redirectors. The Redirectors pass the connection on to the host, allowing you to hide the address of the host from the client users. On Windows NT, Windows 2000, and AIX, the Redirector provides the support for Secure Sockets Layer (SSL) security between clients and the server.

The Redirector acts as a transparent Telnet proxy that uses port remapping to connect Host On-Demand to other Telnet servers. Each defined server is given a local-port number. Instead of connecting directly to the target Telnet server, a Host On-Demand session connects to the Host On-Demand server. The Redirector maps the local-port number to the host-port number of the target and makes a connection.

Redirectors can be connected to each other (in a cascaded configuration). In that case, SSL security is also available between the Redirectors.

The following scenario shows how the Redirector works. Secure connections are possible between the client and Host On-Demand server.

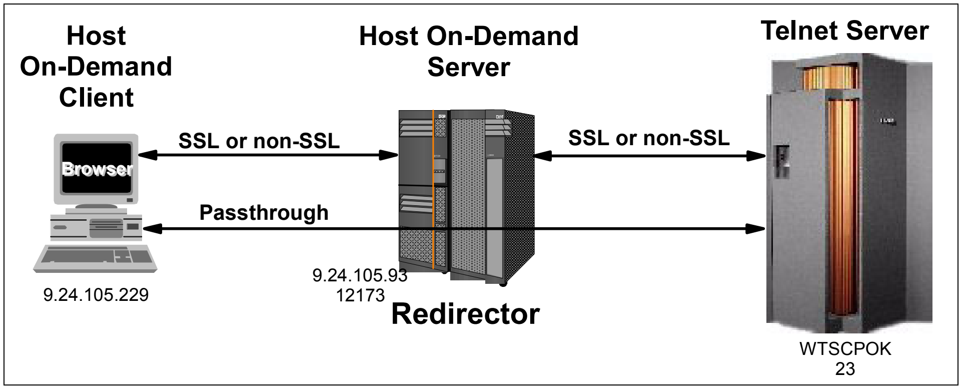


Figure 7-42 How the Redirector works

The Redirector gives Host On-Demand secure access to a wide range of hosts. Typically, a Java applet such as Host On-Demand is made secure by preventing access to all local and network resources except the host that directly supports the applet.

The Redirector sets security for each host. Security choices are no data-stream modification (pass-through), client-side encryption, host-side encryption, and encryption on all data flowing between the Host On-Demand emulator session and the secure server (both).

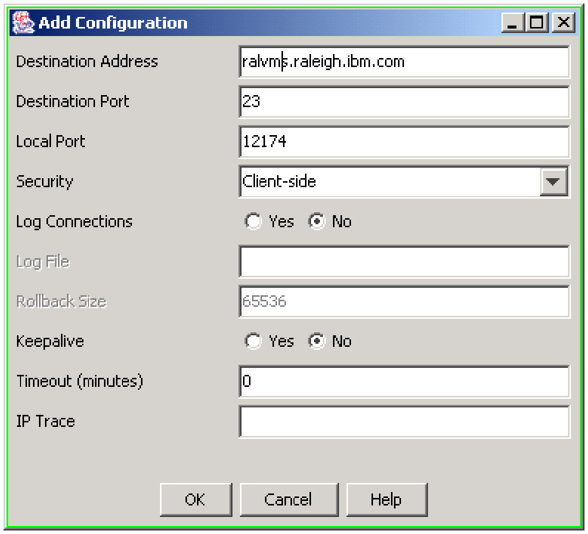
Note: The Redirector service must be started at the Services tab.

7.3.1 Configuring the Redirector

If you are going to use the Redirector, you must create a definition in the Redirector for every destination host to which you want an emulator to connect. It is a good idea to configure it before you configure any sessions, since you must use your Redirector definitions (like destination port) when you configure your sessions. Each definition will consist of the address of the target Telnet server (usually a host system), the port on which that server will listen for Telnet connections, and the port (known as the local port) on which the Redirector will listen for connections (from clients) that are destined for the target server.

To configure the Redirector, follow these steps:

1. Log on as an administrator.
2. Click the **Redirector** task, shown in Figure 7-44.
3. Click **Add** and Figure 7-43 appears.



Destination Address	ralvms.raleigh.ibm.com
Destination Port	23
Local Port	12174
Security	Client-side
Log Connections	○ Yes ● No
Log File	
Rollback Size	65536
Keepalive	○ Yes ● No
Timeout (minutes)	0
IP Trace	

Figure 7-43 Redirector Add Configuration window

4. Type the values for this connection:

   – Destination Address

     The host name or IP address of the target Telnet server. If the IP address is likely to change, use the host name.

   – Destination Port

     The port number for the Telnet server through which it will communicate with the Redirector. Many hosts use the default, which is 23, for Telnet connections.

   – Local Port

     The port number through which the Redirector will communicate with clients.

     Use the standard default port numbers or devise a new numbering scheme. When devising a new scheme, use port numbers that are not already defined for other TCP/IP applications. Because most well-known port numbers are lower than 5000, pick a port number between 5000 and 65535 to avoid conflicts.

   – Security

     Select a security level. Security through the Secure Sockets Layer (SSL) protocol must be set separately for each host configuration. The choices are:

     - None

- Client-side

  Provides encryption of data transmitted between the Redirector and the emulator

- Host-side

  Provides encryption of data transmitted between the Redirector and a secure server (host)

- Both

  Provides encryption of data transmitted through the Redirector, between the emulator and a secure server (host)

  Note that in all connections the data will be decrypted as it enters the Redirector, and re-encrypted as it exits the Redirector. We recommend that if you require end-to-end encryption you use pass-through if both systems will support a direct negotiation of a secure session.

For more details on secure sessions and setting up the Redirector, refer to 11.6, "The Host On-Demand Redirector" on page 446.

See also Chapter 27.1.1, "Example of certificate management" on page 965, which shows an example how to use the HOD Redirector as a proxy for a secure Telnet session with Personal Communications Version 5.7.

– Log Connections

  Select **Yes** if you want to save Redirector connection information in a log file. For each connection from the client, there is a corresponding connection to the host. The log file contains the IP address, port, and the state of the connection. The following table defines the different connection states:

  - **O**: Open
  - **C**: Closed
  - **N**: Not attempted

  If the state of the connection is not attempted, the connection failed to open, or did not attempt to open because of another error; for example, the client connection failed to open, and therefore the host connection was not attempted.

  The default is No. You must stop and restart the Redirector to begin logging connections.

- LogFile

  If you select **Yes** for Log Connections, you can specify a directory and name for the log file. If you do not specify a file name, a window appears asking you to specify a directory and file name. If you do not specify a directory, the system will create the file in /HostOnDemand/lib.

- Rollback Size

  If you select **Yes for Log Connections**, you can specify a maximum size (bytes) for the log file. When the log file reaches the size you specify, any existing Redirector connection information is deleted and new Redirector connection information is logged at the beginning of the file. The default is 65536 bytes.

- Keepalive

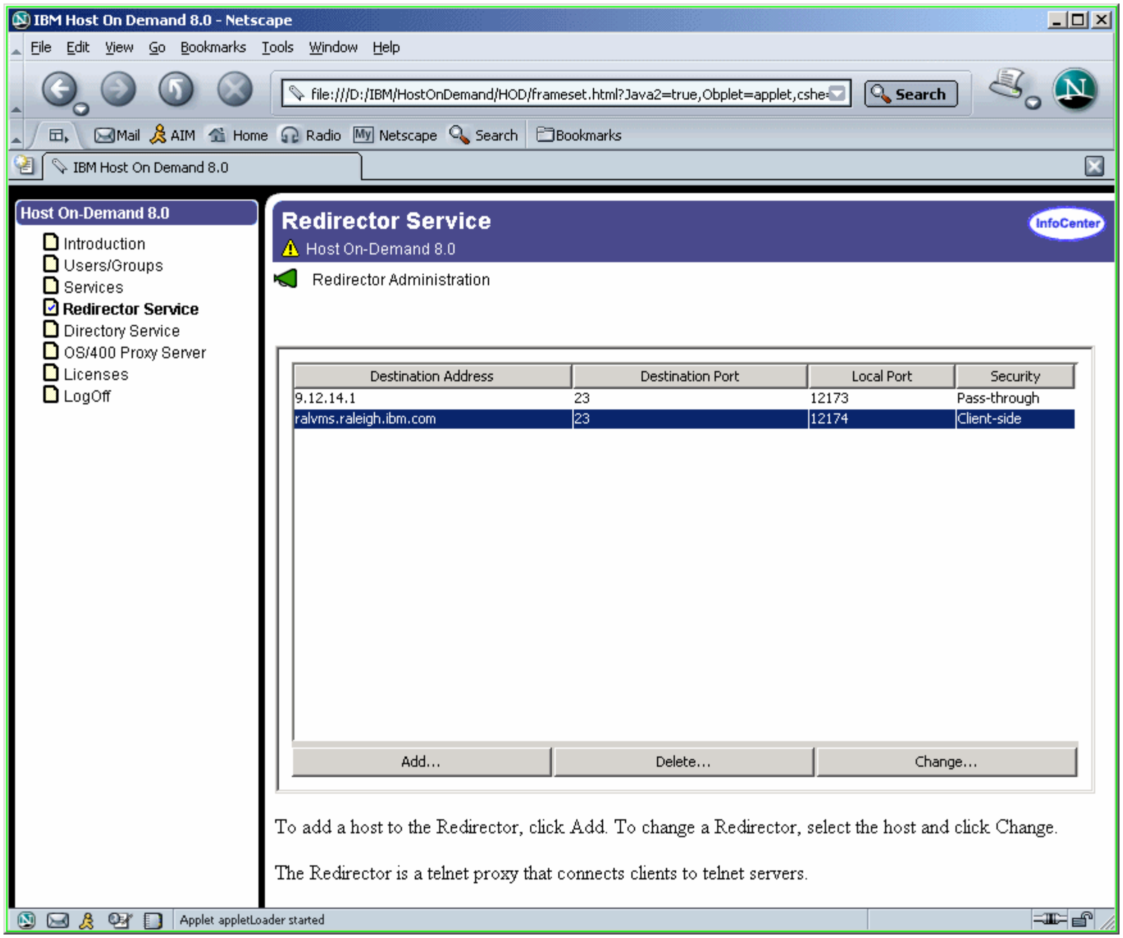
  Select **Yes** if you want the Redirector connection to remain active during a period of inactivity. This parameter forces the TCP/IP stack to send IP-packets regularly, thus keeping the connection active. You must stop and restart the Redirector for Keepalive to take effect.

- Timeout (minutes)

  Specify the number of minutes to wait before dropping an inactive Redirector connection. You must stop and restart the Redirector for the Timeout value to take effect.

- IP Trace

  Type one or more IP addresses of clients you want to trace, separated by commas, to trace the number of bytes sent from the client to the host, and from the host to the client. The trace information is logged in NCoDServices.RAS.txt in the private directory (for example, C:\Program Files\IBM\HostOnDemand\private or /usr/local/hostondemand/private).


IBM Host On Demand 8.0 - Netscape
File Edit View Go Bookmarks Tools Window Help
file:///D:/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=applet,cshe
Search
Mail AIM Home Radio Netscape Search Bookmarks
IBM Host On Demand 8.0
Host On-Demand 8.0
Introduction
Users/Groups
Services
Redirector Service
Directory Service
OS/400 Proxy Server
Licenses
LogOff
Redirector Service
Host On-Demand 8.0
InfoCenter
Redirector Administration
Add...
Delete...
Change...
Applet appletLoader started

Destination Address	Destination Port	Local Port	Security
9.12.14.1	23	12173	Pass-through
ralvms.raleigh.ibm.com	23	12174	Client-side

To add a host to the Redirector, click Add. To change a Redirector, select the host and click Change.

The Redirector is a telnet proxy that connects clients to telnet servers.

Figure 7-44 Redirector administration - two configured connections

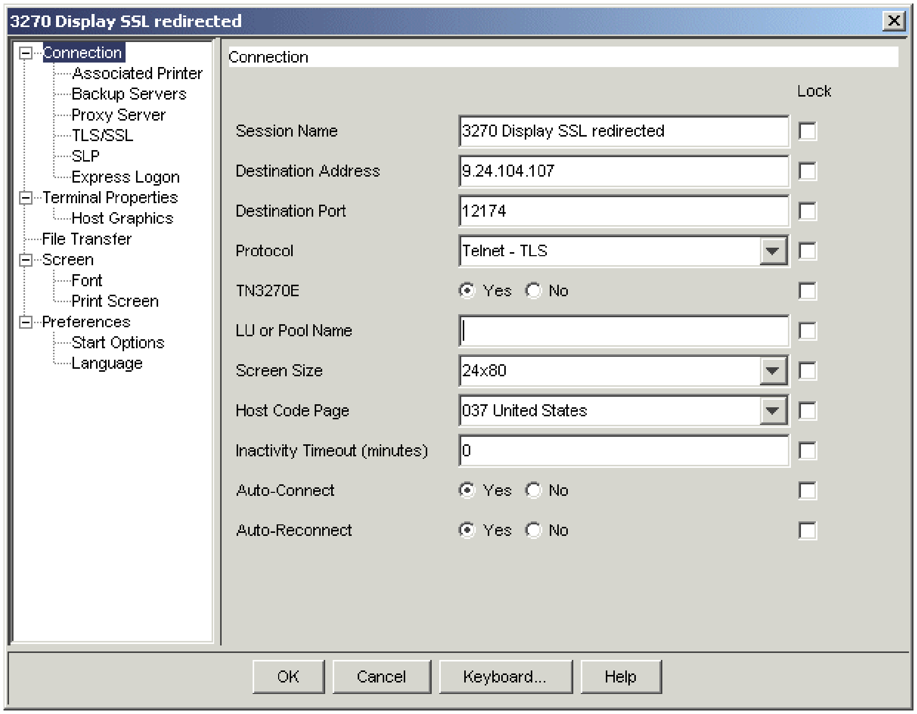
Note: Do not use the Redirector if you do not really need it. It will perform adequately for relatively small numbers of sessions; however, because the Redirector is written in Java, it will not have the performance or capacity that can be obtained by using the Communications Server for AIX or Communications Server for Linux Redirector. See the Readme for recommendations about scalability and max. amounts of users on each platform.

7.3.2 Configuring emulator sessions to use the Redirector

Configuring sessions for the Redirector is like configuring any other session, as described in 7.1.7, “Configuring sessions” on page 277.

Configure a redirected HOD session to RALMVS

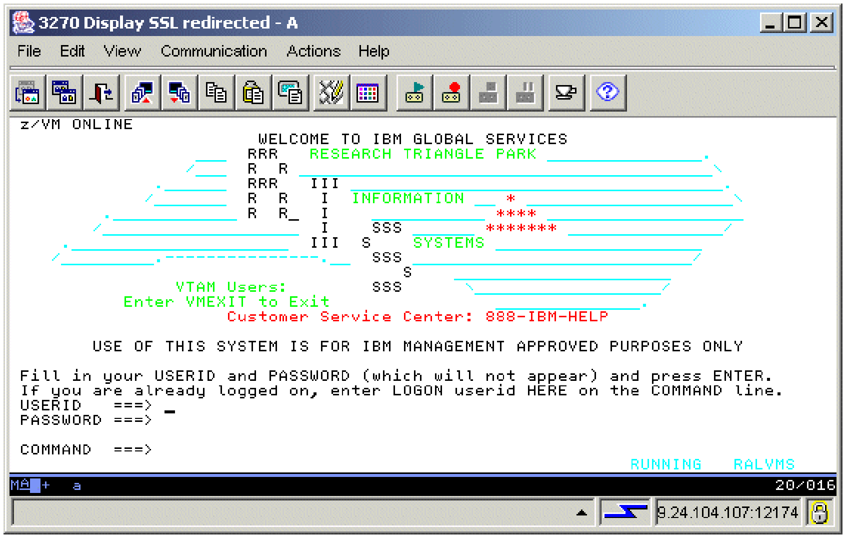
- Click **3270 Display**. In the Configuration notebook, enter the following information as shown in Figure 7-45:
  - Session Name: 3270 Display SSL redirected
  - Destination Address: 9.24.104.107 (the address of the Host On-Demand server, shown in Figure 7-44)
  - Destination Port: 12174 (the local port on the Redirector for this connection, shown in Figure 7-44 on page 344).
  - Protocol: Telnet for non-secured sessions, Telnet - SSL only or Telnet - TLS for secured session (see Help for further information).
  - Click **OK** to save the session.



		Lock
Session Name	3270 Display SSL redirected	□
Destination Address	9.24.104.107	□
Destination Port	12174	□
Protocol	Telnet - TLS	□
TN3270E	● Yes ○ No	□
LU or Pool Name		□
Screen Size	24x80	□
Host Code Page	037 United States	□
Inactivity Timeout (minutes)	0	□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 7-45 Secure session settings for use with Redirector

If you use one of the administration clients with start session enabled, you can point now at your session icon, click the right-click **Start Session**. This will launch the selected session as shown in Figure 7-46. In the lower right corner below the OIA, you see the used IP address and port. This five digit port number makes it obvious that the session is not connected to a TN server, but through a Redirector. The open lock icon next to that indicates that this session does not use security.



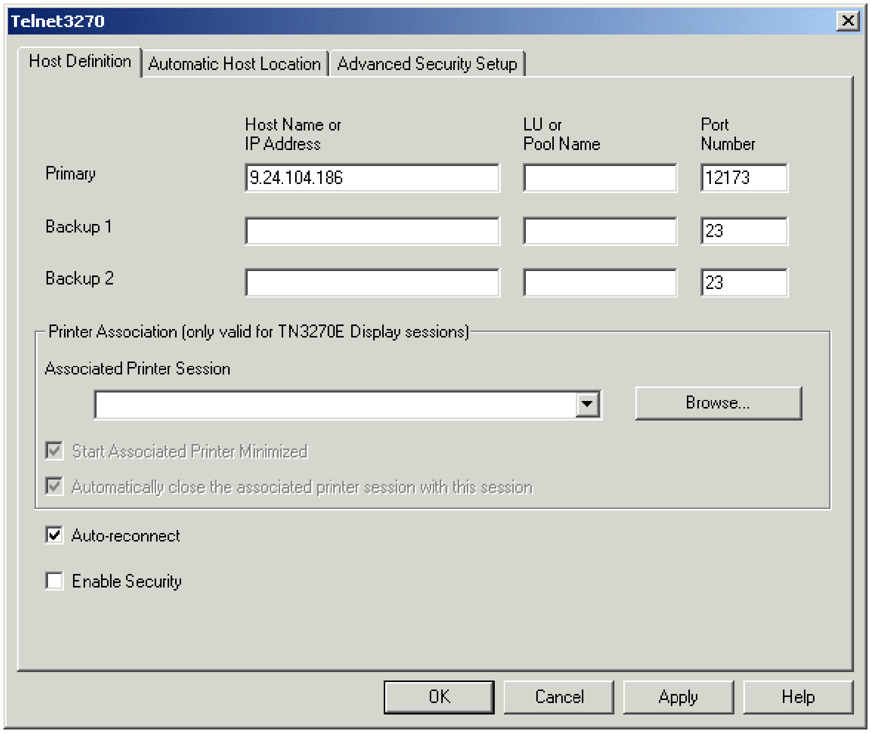
```
z/VM ONLINE
                       WELCOME TO IBM GLOBAL SERVICES
                 ____ RRR    RESEARCH TRIANGLE PARK _______________.
                /____ R  R  _______________________________________\
              .______ RRR    III ___________________________________.
             /_______ R  R    I   INFORMATION __ * ____________________\
          .__________ R  R_   I    ____________ **** ____________________
         /______________________  I     SSS ______ ******* _______________/
      .______________________    III  S    SYSTEMS ____________________
     /_________.----------------.__     SSS ____________________________/
                                          S
                VTAM Users:             SSS  \_____________________/
           Enter VMEXIT to Exit                  ________________.
                     Customer Service Center: 888-IBM-HELP

       USE OF THIS SYSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY

Fill in your USERID and PASSWORD (which will not appear) and press ENTER.
If you are already logged on, enter LOGON userid HERE on the COMMAND line.
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                          RUNNING   RALVMS
MA + a                                                              20/016
9.24.104.107:12174
```

Figure 7-46 Redirected secured HOD session to RALVMS

Configure a redirected PCOMM session

Now we configure a PCOMM client to use the HOD Redirector.

We set up a Personal Communications Telnet session using the IP address and port of our HOD Redirector as shown in Figure 7-47. Note, however, that we configured a different port number (12173) so as to be redirected to a different back-end Telnet server.



	Host Name or IP Address	LU or Pool Name	Port Number
Primary	9.24.104.186		12173
Backup 1			23
Backup 2			23

Printer Association (only valid for TN3270E Display sessions)

Associated Printer Session

☑ Start Associated Printer Minimized

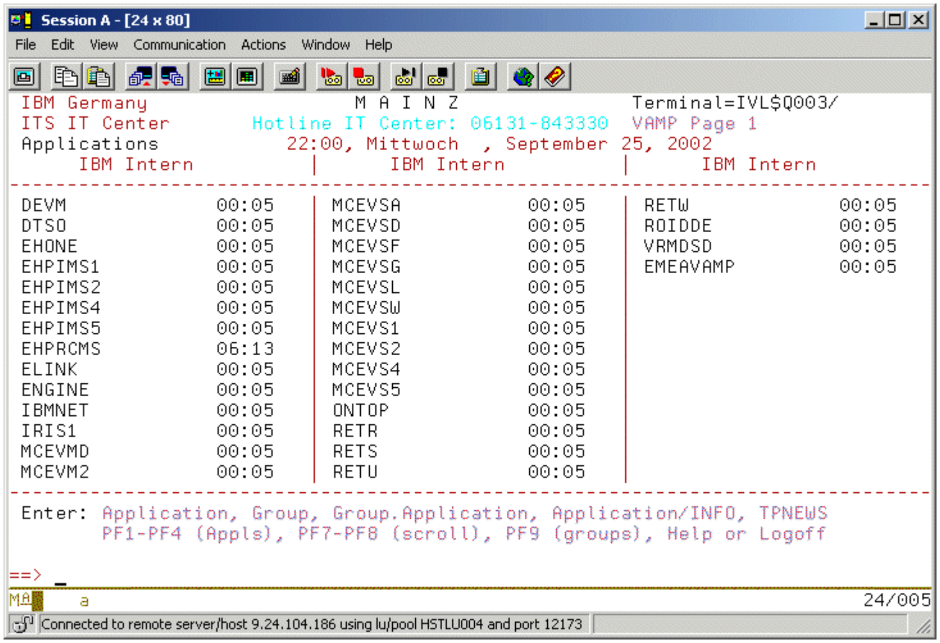
☑ Automatically close the associated printer session with this session

☑ Auto-reconnect

☐ Enable Security

Figure 7-47 PCOMM settings for use with HOD Redirector

Again, we see in the status bar of the emulator the five digit port number, indicating the use of a Redirector as seen in Figure 7-48.



```
 IBM Germany                  M A I N Z               Terminal=IVL$Q003/
 ITS IT Center       Hotline IT Center: 06131-843330  VAMP Page 1
 Applications           22:00, Mittwoch  , September 25, 2002
      IBM Intern          |      IBM Intern          |      IBM Intern
--------------------------------------------------------------------------------
 DEVM             00:05   | MCEVSA           00:05   | RETW             00:05
 DTSO             00:05   | MCEVSD           00:05   | ROIDDE           00:05
 EHONE            00:05   | MCEVSF           00:05   | VRMDSD           00:05
 EHPIMS1          00:05   | MCEVSG           00:05   | EMEAVAMP         00:05
 EHPIMS2          00:05   | MCEVSL           00:05   |
 EHPIMS4          00:05   | MCEVSW           00:05   |
 EHPIMS5          00:05   | MCEVS1           00:05   |
 EHPRCMS          06:13   | MCEVS2           00:05   |
 ELINK            00:05   | MCEVS4           00:05   |
 ENGINE           00:05   | MCEVS5           00:05   |
 IBMNET           00:05   | ONTOP            00:05   |
 IRIS1            00:05   | RETR             00:05   |
 MCEVMD           00:05   | RETS             00:05   |
 MCEVM2           00:05   | RETU             00:05   |
--------------------------------------------------------------------------------
 Enter: Application, Group, Group.Application, Application/INFO, TPNEWS
        PF1-PF4 (Appls), PF7-PF8 (scroll), PF9 (groups), Help or Logoff

==> _
MA    a                                                                   24/005
```

Connected to remote server/host 9.24.104.186 using lu/pool HSTLU004 and port 12173

Figure 7-48 Personal Communications uses HOD Redirector

7.4 Directory service

Enterprise customers often need to manage Host On-Demand user and group configuration information for a large number of users. For reasons of performance or administrative convenience, the information for these users may be distributed and managed across multiple Host On-Demand servers. Unfortunately, the user information is not shared among the Host On-Demand servers, or among those servers and other applications.

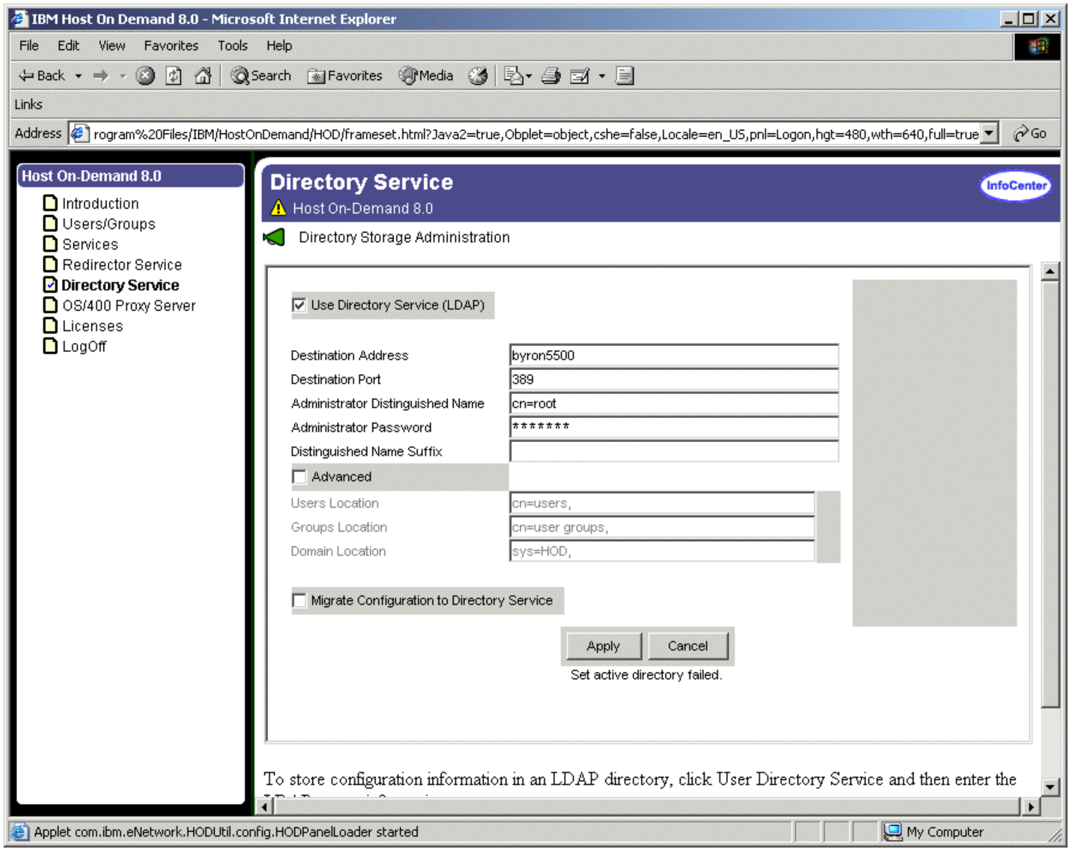
However, a directory service, such as that provided by a Lightweight Directory Access Protocol (LDAP) server, can enable this kind of information sharing. For example, a single LDAP directory can store configuration information for multiple Host On-Demand servers. Configuration information is stored in directory entries in an LDAP directory; these entries are uniquely identified by a distinguished name (DN).

With Host On-Demand, you can use an LDAP directory instead of using the Host On-Demand server's private data store to store user, group, and session information. This option is available from the Directory Service in the Host On-Demand Administration window.

> **Note:** Migrating to LDAP has significant implications for your group and user configuration information. Make sure you understand these implications before you migrate. See “Implications of migrating to LDAP” on page 351.

When configuring a Host On-Demand server for use with an LDAP directory server, select the **Directory Service** task from the navigation area, and you will be presented with the window shown in Figure 7-49. This window will allow you to enable/disable LDAP directory service, identify the directory server and suffix that you want to use, and optionally let you migrate your existing Host On-Demand configuration data to the LDAP directory server. Regardless of whether or not you migrate, the default administrator ID will be created in the directory server with the default user ID/password of `admin/password`.

A detailed description of the LDAP directory and its usage can be found in Chapter 8, “LDAP directory server” on page 373.



rogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true

☑ Use Directory Service (LDAP)

Destination Address	byron5500
Destination Port	389
Administrator Distinguished Name	cn=root
Administrator Password	*******
Distinguished Name Suffix	

☐ Advanced

Users Location	cn=users,
Groups Location	cn=user groups,
Domain Location	sys=HOD,

☐ Migrate Configuration to Directory Service

Apply Cancel

Set active directory failed.

To store configuration information in an LDAP directory, click User Directory Service and then enter the

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 7-49 Directory Service administrator

7.4.1 Use Directory Service (LDAP)

To configure Host On-Demand to use an LDAP directory, complete the following fields on the Directory tab in the Host On-Demand administration window:

- Destination Address

  Type the IP address of the LDAP directory. Use either the host name or dotted decimal format. The default is the IP address of the Host On-Demand server.

- Destination Port

  Type the TCP/IP port on which the LDAP server will accept a connection from an LDAP client. The default port is 389.

- Administrator Distinguished Name

  Type the distinguished name (DN) of the directory administrator that allows Host On-Demand to update information. You must use the LDAP string representation for distinguished names (for example, cn=root).

- Administrator Password

  Type the directory administrator's password.

- Distinguished Name Suffix

  Type the distinguished name (DN) of the highest entry in the directory information tree (DIT) for which information will be saved. Host On-Demand will store all of its configuration information below this suffix in the DIT. You must use the LDAP string representation for distinguished names (for example, o=ibm,c=us).

Under normal circumstances it is recommended that you do not change anything in the Advanced section of this window. The only time you should consider enabling and modifying the Advanced section is if you were connecting to an LDAP directory server, and trying to use previously installed directory entries that used the IBM ePerson schema.

7.4.2 Migrate configuration to LDAP directory

To migrate users and groups to an LDAP directory, click **Directory Service** in the Administration window, check the **Migrate Configuration to Directory Service** box and click **Apply**.

If a group or user already exists in the LDAP directory, the information from the Host On-Demand data store is not written for that particular group or user. Also, if a user is a member of multiple groups in the Host On-Demand data store, the user will be assigned to only one of those groups in the LDAP directory.

During migration, log messages are written to standard output, which is typically the browser's Java console. Additionally, the log messages are saved in a log file (hodldap.log) in the private directory of the Host On-Demand server.

If the migration program ends prematurely, for example, because of a network failure, you can select this option and run the migration program again. After successful migration, the Migrate Configuration to Directory Service checkbox is automatically cleared. Simply select it and click **Apply**, and the migration process will begin again.

Once you have switched to the LDAP directory server, subsequent user-related changes will be made only in the LDAP directory, including administrative changes to groups, users, or sessions, and changes such as new passwords, macros, or keyboard changes, by either the administrator or a user.

Implications of migrating to LDAP

This section contains important information about using Host On-Demand with LDAP. You should read and understand this section before using LDAP.

LDAP enables you to manage Host On-Demand configuration information by arranging those users into a hierarchical tree of groups. A group can have one of more subgroups as children and each subgroup inherits all of the sessions defined by the parent group. A user can be an immediate member of any one group, and inherits sessions from all the groups in its inheritance tree. This means that you can define sessions in a high-level group for a large number of users and subgroups, and then customize them in lower-level groups for smaller numbers of users. It also means that no user can belong to more than one group.

- Will migrating to LDAP change my present group structure and user configurations?

  Yes. Because your Host On-Demand private data store is not arranged hierarchically, migrating your configuration information to an LDAP directory changes the relationship between your users and groups. Specifically, all groups and their sessions become children of the root group of the LDAP directory, and all users become members of one of the groups they were members of before migration (refer to the migration log for details). Also, because of this change, users that are members of multiple groups will lose configuration information as a result of migration.

- What happens if I choose not to migrate my configuration information?

  None of the users, groups, and sessions that are defined in the private data store will be accessible from the logon window or the administration window. If it does not already exist, Host On-Demand will create a single administrator User ID named "admin" with a password of "password".

- What happens to the configuration information in the private data store when I migrate?

  It is preserved and is not modified by the migration process. However, it does not reflect the latest updates either. When you use an LDAP directory, changes to configuration information will only be updated in that LDAP directory.

- Once I have migrated and started using LDAP, how do I switch back to using the Host On-Demand private data store?

  Clear the Use Directory Service (LDAP) box on the Directory tab, and click **Apply**. This will disable use of the LDAP directory and Host On-Demand will begin retrieving user and group information from the private data store.

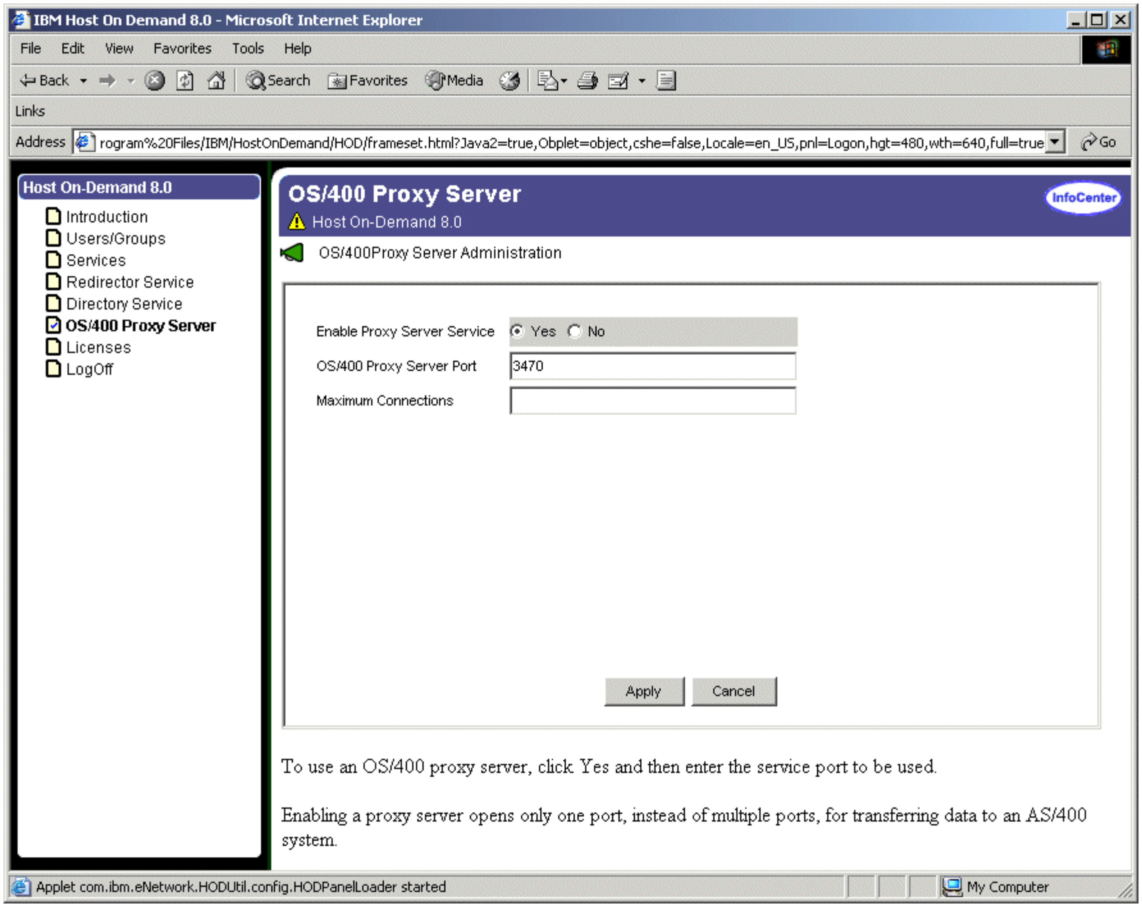
- Is there anyway to migrate my configuration back to the Host On-Demand private data store?

  No, migrating from an LDAP directory to the Host On-Demand private data store is not supported.

7.5 OS/400 Proxy Server

On AS400 sessions, a file transfer session opens a new port on the AS/400 and builds a new additional session to support it. The Host On-Demand OS/400 Proxy Server is used to channel all those file transfer ports through only one port. Using one port reduces the security risk when transferring files through a firewall. For details on using OS/400 Proxy Server refer to Chapter 10., “OS/400 Proxy” on page 397.

To enable/disable and configure the O/S400 Proxy Server, you must click the **OS/400 Proxy Server** task in the HODAdmin.html navigation window (refer to Figure 7-41 on page 337). This brings up the window shown in Figure 7-50.



Address: rogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true

OS/400 Proxy Server

Host On-Demand 8.0

OS/400Proxy Server Administration

Enable Proxy Server Service ● Yes ○ No

OS/400 Proxy Server Port: 3470

Maximum Connections:

To use an OS/400 proxy server, click Yes and then enter the service port to be used.

Enabling a proxy server opens only one port, instead of multiple ports, for transferring data to an AS/400 system.

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 7-50 OS/400 Proxy Server Administration

To enable the OS/400 Proxy Service, select the **Yes** radio button. This enables the remaining fields on this window. You may specify the port you wish the proxy to use (default is 3470). The Maximum Connections field allows you to limit the number of connections; however, unless you are experiencing problems we recommend you leave this blank. You must click **Apply** to make the selections active.

7.6 License Use Management

A Host On-Demand server keeps a count of the number of concurrent users at any given time. This enables you to determine and validate the number of Host On-Demand licenses that you need.

The number of concurrent users is based on a user’s ID and IP address. Locally installed clients are not included in this count. Any of the following combination of sessions is counted as a single use:

- HACL or Beans sessions
- Emulator sessions
- Database On-Demand sessions

A license is considered to be in use from the time a session is started until it is closed, regardless of any pattern of usage during that period. If more than one session is active from the same combination of IP address and user ID, only one client is counted.

Click **Licenses** in the Administration window (see Figure 7-1 on page 267).The Licenses window shown in Figure 7-51 will appear.

You must click **Apply** to activate any changes that you make.

To take advantage of the license usage support with Host Access Class Library (HACL) and Host Access Bean programs, you must install a Host On-Demand server (from which the programs must be downloaded) and properties must be passed to the ECLSession constructor or session bean. Valid properties are:

- The type of server that will manage usage. The property name is defined by the constant ECLSession.SESSION_LUM_LICENSING, and the value must be HOD.
- The identity of the Host On-Demand server. The property name is defined by the constant ECLSession.SESSION_SERVICE_MGR_HOST, and the value must be the host name or IP address of the Host On-Demand server.
- The identity of the user. In multi-user environments, use the User ID property to further refine license-usage counting. This property name is defined by the constant user ID, and the value must be a string that uniquely defines a user in a multi-user environment.

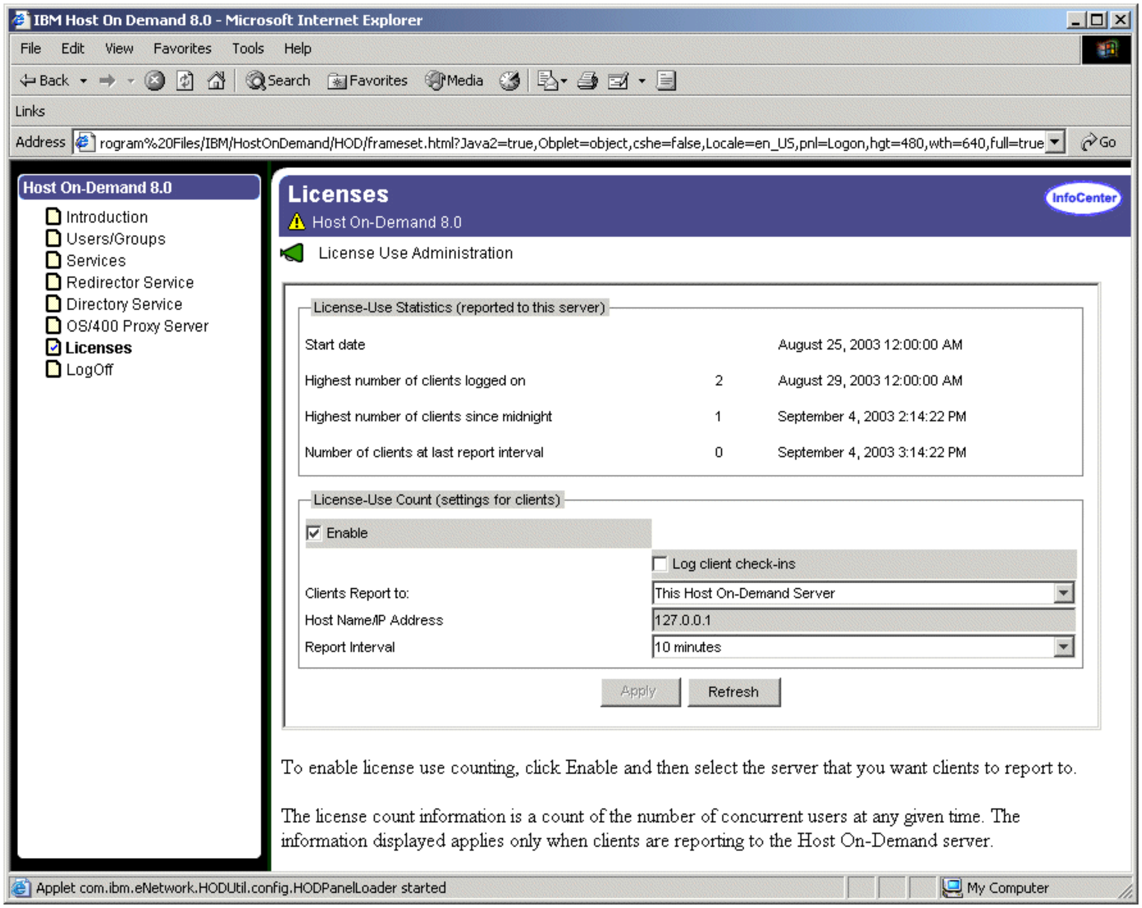
7.6.1 Enabling License-Use Count

Host On-Demand counts the sessions when the **Enable** checkbox in License-Use Counts (settings for client) is selected. To stop the counting, clear the checkbox. However, this does not stop HTML-based clients from sending a continuous`I am here` message to the configuration servlet (default port is 8999) as defined in Report Interval. To prevent html-based clients from sending this heartbeat, see 7.6.3, “Disabling License-Use Count” on page 357.

If you enable **Log Client Check-ins**, the HOD server triggers a log entry for every client report received by the configuration server. The log entry content enables you to track the activity of individual users. Each entry records:

- appropriate timestamp (formatted for your locale)
- IP address of the client
- Host On-Demand userID, if applicable (because users of the HTML model do not have individual Host On-Demand user IDs, they are assigned the generic label *HTML*.)

Host On-Demand writes these entries to files every twenty-four hours at midnight. It names the files according to date, and stores them in the private directory.



Address: rogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true

Licenses

Host On-Demand 8.0

License Use Administration

License-Use Statistics (reported to this server)

Start date		August 25, 2003 12:00:00 AM
Highest number of clients logged on	2	August 29, 2003 12:00:00 AM
Highest number of clients since midnight	1	September 4, 2003 2:14:22 PM
Number of clients at last report interval	0	September 4, 2003 3:14:22 PM

License-Use Count (settings for clients)

☑ Enable

□ Log client check-ins

Clients Report to: This Host On-Demand Server

Host Name/IP Address 127.0.0.1

Report Interval 10 minutes

To enable license use counting, click Enable and then select the server that you want clients to report to.

The license count information is a count of the number of concurrent users at any given time. The information displayed applies only when clients are reporting to the Host On-Demand server.

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 7-51 Licenses window

- Clients Report to

Use the drop-down menu to select whether the clients should report to this or another Host On-Demand server. If you select **Other Host on Demand Server** you need to overwrite the Host Name/IP Address field as well.

The support for License-Use Management (LUM) servers has been removed.

- Host Name/IP Address

  Type the host name of the Host On-Demand that clients should report to. (select first **Other Host on Demand Server** in the drop down list from the **Clients Report to** parameter).

- Report Interval

  Select the amount of time for clients to wait between sending a `I am here` message to the specified server. Clients begin using a new interval once the previous interval has expired.

7.6.2 License Use Statistics

This information applies only when clients are reporting to this Host On-Demand server.

Clients can be switched to report to this or any other Host On-Demand server at any time. However, the clients that are already connected are not switched until they have logged off or closed the browser and reconnected:

- Start date

  The date and time that the first check was performed.

- Highest number of clients logged on

  The highest number of concurrent users logged on since the start date, and the date and time that this occurred. The overall information is saved in a file named LicenseOverallHistory.txt in the \private directory. This file contains one entry per day showing the highest number of users each day since the start date, and is continuously appended until it is deleted or renamed.

- Highest number of clients since midnight

  The highest number of users since midnight, and the date and time that this occurred.

- Number of clients at last report interval

  The number of users when the last count was performed, and the date and time this occurred. The information is saved in a file named LicenseRecentHistory.txt in the \private directory. This file contains entries for the last 12 counts.

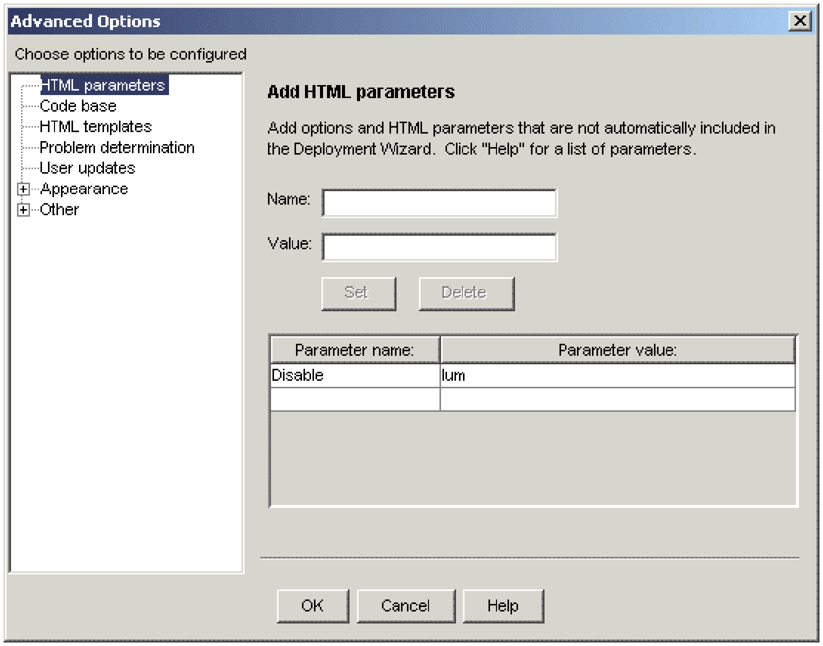
7.6.3 Disabling License-Use Count

You may disable the client from performing license use tracking activities in one of three ways:

1. For those users who log into the Host On-Demand configuration server, license use tracking may be disabled by clearing the Enable checkbox on the Licenses window shown in Figure 7-51.
2. Clients created with the Deployment Wizard may disable license use counting by adding the following parameter to the HTML file:

   ```
   <Param Name=Disable Value=LUM>
   ```

   See Figure 7-52.



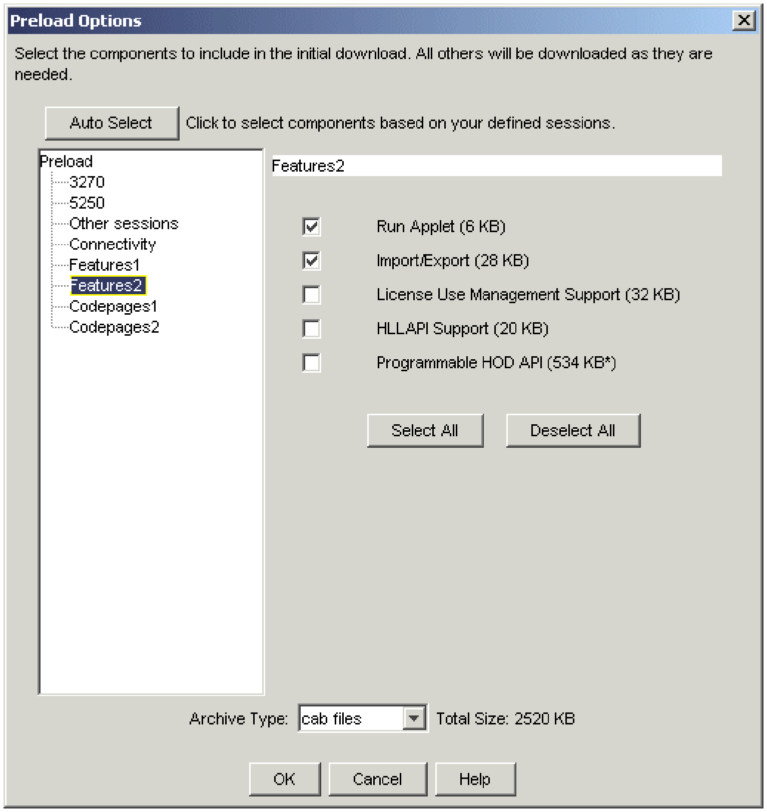
Add options and HTML parameters that are not automatically included in the Deployment Wizard. Click "Help" for a list of parameters.

Parameter name:	Parameter value:
Disable	lum

Figure 7-52 Disable License-Use Count with the Deployment Wizard

When using the Deployment Wizard, it is also recommended that you clear the License Use Management checkbox from the preload configuration window as shown in Figure 7-53. This stops the downloading of class file(s) that perform license use tracking. This also makes for a smaller client.

Important: When using an HTML file created with the Deployment Wizard, your configuration servlet port (default is 8999) is closed at your firewall, and you have not disabled the license use counting as described above, the users will experience a noticeable delay when starting their sessions.



Preload Options

Select the components to include in the initial download. All others will be downloaded as they are needed.

Click to select components based on your defined sessions.

Features2

☑ Run Applet (6 KB)

☑ Import/Export (28 KB)

□ License Use Management Support (32 KB)

□ HLLAPI Support (20 KB)

□ Programmable HOD API (534 KB*)

Archive Type: cab files Total Size: 2520 KB

Figure 7-53 Licences management in pre-load options of Deployment Wizard

7.7 Directory Utility

Directory Utility is a command-line Java application an administrator can use to manage user, group, or session configuration information. This information is stored either in the Host On-Demand default data store, or in an LDAP directory. This utility is only useful in the environment where the configuration server-based model or the combined model is in use (refer to 13.1, “Host On-Demand configuration models” on page 502). Directory Utility allows you to add, delete, or update large numbers of users, groups, or sessions in a batch mode environment instead of using the Administration client. Directory Utility reads an XML ASCII file that contains the following actions to be performed on users, groups, or sessions defined to the configuration server:

- Add, update, and delete groups
- Add, update, and delete users from groups
- Add, update and delete sessions from users or groups

7.7.1 Using Directory Utility

On Windows NT and Windows 2000, the command file to run Directory Utility and a sample XML file are located in the HostOnDemand\lib\samples\DirUtil directory. The command file is called DirUtil.cmd, and the sample text file is called Sample.xml.

The command, or script file for other operating systems and the sample XML file are located in the HostOnDemand\lib\samples\DirUtilCommandFiles directory. The sample text file is called Sample.xml. The command or script files are shown in Table 7-2.

Table 7-2 Directory Utility command files

Operating system	**File name**
Windows	DirUtil.cmd
AIX	DirUtil-AIX
Novell	DirUtil-Novell.ncf
OS/2	DirUtil-OS2.CMD
UNIX, HP-UX, Linux, and Solaris	DirUtil-UNIX
iSeries	DirUtil-AS400.sh
zSeries	DirUtil-S390

To run Directory Utility, type the following at the command line:

```
DirUtil-xxx filename.xml admin password [hostname] [port] [CON | FILE]
```

Important: The parameters are positional, not keyword; therefore, the order of the parameters is important.

Where:

`DirUtil-xxx` Directory Utility command or script file for your operating system; see Table 7-2.

`filename.xml` The file that contains the XML elements to manage users, groups, and sessions. The text file must have an .xml extension, and be a valid XML file. Refer to 7.7.3, “General XML file syntax” on page 362 for a description of the XML file commands. If the text file is not in the same directory as the Directory Utility command file, you must specify the path to the file. This parameter must be present on the command line.

`admin` Is the Host On-Demand administrator’s user ID. This parameter must be present on the command line.

`password` Is the Host On-Demand administrator's password. This parameter must be present on the command line.

`[hostname]` The Host On-Demand Service Manager's host name or IP address. The default host name is localhost (127.0.0.1). This parameter is optional.

`[port]` The Host On-Demand Service Manager's port. The default Service Manager port is 8999. This parameter is optional.

`[CON | FILE]` Determines how messages will be logged and displayed. If the command line contains the string CON, messages will go only to the console. If the command line contains the string FILE, messages will only be written to a log file. If neither string is included (the default), the messages will be written to the console, and also to a log file. The name of the log file is based on the name of the XML file. If your XML file name is myxmlfile.xml, then your log file name is myxmlfile.log.

Note: The Host On-Demand Service Manager must be running on the Host On-Demand server specified by hostname in order for the Directory Utility to update Host On-Demand or LDAP configuration information.

7.7.2 The Directory Utility list action

The Directory Utility (DirUtil) list action is new in Host On-Demand Version 8.

It allows administrators listing and searching of users/groups:

- Listing

  List user and/or group specific information

- Searching

  Search users and/or groups and allows wildcards (*) to locate matching strings.

The supported parameters are:

<userid>, <groupid>, <filename>

Any of them may be omitted.

The output is in XML and can be used (with changes) as input for a sequencing DirUtil action. The default name for the output file is DirUtilList.xml).

Example for the list action

The administrator would like to list all users with username that starts with `m` and creates the following xml-file as shown in Figure 7-2.

Example 7-2 List all usernames starting with m

```
<!DOCTYPE dirscript[ ... ]>

<dirscript>
   <action type = "list">
      <userlist>
         <userid>m*</userid>
         <groupid>*</groupid>
      </userlist>
      <grouplist>
         <groupid>*</groupid>
         <filename>c:\temp\out.xml</filename>
      </grouplist>
   </action>
</dirscript>
```

Then he goes to C:\Program Files\IBM\HostOnDemand\lib\samples\DirUtil and runs:

```
DirUtil lisusr.xml admin password
```

The output file C:\temp\out.xml looks like what is shown in Example 7-3.

Example 7-3 Output file

```
<!DOCTYPE dirscript[ ... ]>
   <!-- <userlist> -->
   <!--     <userid>m*</userid> -->
<!--     <groupid>*</groupid> -->
   <!-- </userlist> -->
<dirscript>
   <action type = "list">
            <user>
                  <userid>matthew</userid>
         <groupid>USERS</groupid>
                  <description></description>
                  <authentication>pw</authentication>
            </user>
            <user>
                  <userid>martin</userid>
                  <groupid>USERS</groupid>
                  <description></description>
                  <authentication>pw</authentication>
            </user>
      </action>
</dirscript>
```

7.7.3 General XML file syntax

The descriptions of the elements below describe the format for valid XML elements that can be included in the Directory Utility XML control file. A basic understanding of XML is assumed. Note that comment lines begin with an `<!--` and end with `-->`. All elements are case sensitive.

You must use an ASCII editor that generates valid unicode characters, such as the Windows Notepad or WordPad editors. If you receive the error `DIR0037 Fatal error: Invalid XML Character while using the XML file with Directory Utility`, the ASCII editor did not generate valid Unicode characters. Use a different ascii editor that does generate valid Unicode characters.

The XML elements and their structure is shown in Example 7-4 followed by a description of each element.

Example 7-4 XML elements and structure

```
<dirscript>
    <action>

        <group>
            <groupid>
            <description>
            <parent>
            <removeusers>

        <user>
            <userid>
            <groupid>
            <description>
            <authentication>
                <pw>
                <nativeid>
            <savepref>

        <session>
```

```
            <filename>
            <groupid>
            <userid>
            <description>
```

<dirscript>

The root element in the XML file that contains all the other elements and identifies the document as one that can be processed by Directory Utility is <dirscript>.

- Attributes: none
- Required elements: <action type=xxx>
- Optional elements: none

<action type=xxx>

This element identifies the action to be performed on the elements enclosed in the <action> element. You can have multiple action elements within the <dirscript> element. Elements placed outside either the <dirscript> element or this element in the XML file are ignored by Directory Utility.

Valid action types are:

- Add
- Delete
- Update
- List

  The action type *list* is new in Host On-Demand Version 8.

At least one of the following elements is required within the <action> element:

- <group>

  This element identifies the group that is affected by the action. If the action is **`add`** and the group already exists, you will receive a message that the group is a duplicate.

- <user>

  This element identifies the user that is affected by the action. If the action is **`add`** and the user already exists, you will receive a message that the user is a duplicate.

- <session>

  This element identifies the session that is affected by the action. The session element is not valid when the action is **`update`**. If the session already exists, a new session named **`1:description`** is added, in the same way that the Administration client adds a duplicate session.

<group>

There is only one required element, a Unicode text string that identifies the group. If you are using Host On-Demand, the <groupid> is converted to uppercase when the group is added. If you are using LDAP, the <groupid> can be mixed-case.

The optional elements are:

- <description>
- <parent>
- <removeusers>

<description>

This element is a unicode text string that describes the group, and is only valid when the action type is **`add`** or **`update`**.

<parent>

This element identifies the parent of this group. This element is only valid when the action is **`add`** or **`update`**, and when using LDAP. If this element is not specified when the action is **`add`**, the group is added to the top level.

<removeusers>

This element allows you to delete all the users that belong exclusively to this group when you delete the group. This element is only valid when the action is **`delete`**, and this element is not valid when using LDAP. Valid values are Yes and No. If `Yes` is specified, then the users in this group will be deleted when the group is deleted. If `No` is specified and there are users in the group, the users that belong only to this group are moved to the HOD group and the group is deleted.

The default is No.

If you have many users, it may take some time for the processing of this element to complete.

<user>

This is the enclosing element in defining a user.

Attributes: none

The following elements are required:

- <userid>

  This is the identifier that defines the user. This element is always required. If you are using Host On-Demand, the <userid> is converted to lowercase. If you are using LDAP the <userid> can be mixed-case.

- <groupid>

  This element defines the group to which the user is being added. This element is required when the action type is **`add`** and ignored when the action type is **`delete`**. If you are not using LDAP, you can specify multiple <groupid> elements. If you are using an LDAP directory, a user can exist in only one group; therefore, if you specify multiple groups, an error message will be generated and the user is not added. Groups specified must exist before you can add users to them. If the action type is **`update`**, the user is updated to have membership in this group.

The following elements are optional:

- <description>

  A unicode text string that describes the user.

- <authentication type=xxx>

  Specifies the type of authentication that is used for the user. Valid types are **`native`** and **`pw`**. If this element is omitted, no authentication will be configured for the user.

- <savepref>

  Specifies if the user is authorized to save preferences (changes that the user might make to a host session configuration). Valid values are Yes or No. If this element is not specified, the default of Yes will be used.

- <removegroupid>

  You can update a user so that they no longer have membership in a specified group. This element is only valid if the action type is **`update`**. You must use a valid <groupid> that contains this user.

<authentication type=xxx>

This element specifies the authentication used for the user. You can use password authentication, or Native Authentication if the Service Manager is using an LDAP directory. No authentication will be configured for the user if this element is not specified when the action type is add, or if **native** is selected and you are not using an LDAP directory.

Valid values are:

- pw
- native

The following element is required:

- <nativeid>

The value specified here is the ID of the user on the native operating system. This element is required and valid only when using LDAP directory and when the authentication type is **native**.

The following elements are optional:

- <pw>

  The value entered is the password associated with the user. This element is only valid when the authentication type is **pw**.

- <changepw>

  Specifies whether or not the user is authorized to change his password. Valid values are Yes or No. If this element is omitted a default of Yes is set for the user, enabling the user to change their password. This element is only valid if the authentication type is **pw** and is ignored if the authentication type is **native**.

<session>

This element defines a session available to the user.

The required elements to define the session are:

- <filename>

  This element specifies the file containing the session definition. The session definition file may be created by using the Export Session menu option from any defined Host On-Demand session. The default file extension for session files is .hod. If the file does not exist in the directory from which Directory Utility is run, then the <filename> element should contain the full path to the session file, and it is only required when adding a session.

- <description>

  The description is a unicode text string that describes the session and is used as the session name. The <description> is required to update or delete a session. If <description> is omitted, the session name will be used for the description of the file.

At least one of the following element types is required:

- <userid>

  The user identifier for the user to which this session is being added. User IDs must already exist before the session can be added. You can include multiple <userid> elements to add this session for multiple users.

- <groupid>

This element specifies the identifier for the group to which the session is being added. Groups must already exist before the session can be added. You can include multiple <groupid> elements to add a session for multiple groups.

Note: You can specify multiple users or multiple groups in the session element, but you cannot specify both users and groups in the same session element.

7.7.4 Example

This example illustrates how to take the objective of the bulk update, translate the requirements into the required XML file format, and run Directory Utility.

Objectives

The objectives of this example are to add the following groups and users:

- Management
  - Authentication: none
  - Members:
    - Joe Cline (jcline)
    - John Bird (jbird)l
  - One session at the group level: WTSCPOK
- ProjectLeaders
  - Place under the Management group
  - Authentication: Host On-Demand password
  - Members:
    - George Baker (gbaker)
    - David Russell (drussell)
    - Steve Watts (swatts)
- Residents
  - Authentication: Native Authentication
  - Members:
    - Anna O’Neal (bogardus)
    - Sriram M R (cohen)
    - Anna Murphy (agoneal)

Next, the following sessions must be available to the indicated groups. The session definitions were previously created by the administrator using the Export Session option from the graphical administrative interface and stored in the same directory as the utility command file and sample XML file.

- Management

  - WTSCPOK

- ProjectLeaders
  - WTSCPOK
  - MVS03a
- Residents
  - MVS03a
  - HODAIX

Finally, a single session, HODLinux, is added for user George Baker.

Sample XML file

Example 7-5 illustrates the XML file that was used.

Example 7-5 ITSOSample.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Begin DTD - The DTD should not be modified.-->
<!DOCTYPE dirscript [
<!ELEMENT dirscript (action)+>
<!ELEMENT action (group | user | session)+>
<!ELEMENT group (groupid, description?, parent?, removeusers?)>
<!ELEMENT user (userid, groupid*, description?, authentication?, savepref?,
removegroupid?)>
<!ELEMENT session (filename?, (groupid | userid)+, description?)>
<!ELEMENT groupid (#PCDATA)>
<!ELEMENT userid (#PCDATA)>
<!ELEMENT description (#PCDATA)>
<!ELEMENT parent (#PCDATA)>
<!ELEMENT removeusers (#PCDATA)>
<!ELEMENT removegroupid (#PCDATA)>
<!ELEMENT authentication ((pw?, changepw?) | (nativeid))>
<!ELEMENT pw (#PCDATA)>
<!ELEMENT changepw (#PCDATA)>
<!ELEMENT nativeid (#PCDATA)>
<!ELEMENT savepref (#PCDATA)>
<!ELEMENT filename (#PCDATA)>
   <!ATTLIST action type (add | delete | update) #REQUIRED>
   <!ATTLIST authentication type (pw | native) #REQUIRED>
]>
<!-- End DTD -->

<dirscript>
   <action type="add">
        <!-- Add three groups, Management, Project Leaders, Residents  -->
      <group>
         <groupid>Management</groupid>
         <description>ITSO Managers</description>
      </group>
      <group>
         <groupid>ProjectLeaders</groupid>
         <description>ITSO Project Leaders</description>
         <!-- the parent element should only be specified if using LDAP -->
         <parent>Management</parent>
      </group>
      <group>
         <groupid>Residents</groupid>
         <description>SG24-6182 Residents</description>
      </group>

        <!-- The following sessions were previously exported and reside in the 
executing
      directory: WTSCPOK.hod, HODAIX.hod, HODLinux.hodm MVS03a.hod -->

        <!-- Add a session to the Management group -->
      <session>
         <description>WTSCPOK</description>
         <filename>WTSCPOK.hod</filename>
         <groupid>Management</groupid>
      </session>

        <!-- Add a sessions to the Project Leaders group -->
      <session>
         <description>MVS03a</description>
         <filename>MVS03a.hod</filename>
         <groupid>ProjectLeaders</groupid>
      </session>

        <!-- Add a sessions to the Residents group -->
      <session>
         <description>HODAIX</description>
         <filename>HODAIX.hod</filename>
         <groupid>Residents</groupid>
      </session>
      <session>
         <description>MVS03a</description>
         <filename>MVS03a.hod</filename>
         <groupid>Residents</groupid>
      </session>
      <session>
         <description>MHODLinux</description>
         <filename>HODLinux.hod</filename>
         <groupid>Residents</groupid>
      </session>

        <!-- Add Management users, no passwords -->
      <user>
         <userid>jcline</userid>
         <description>Joe Cline</description>
      <!-- note the authentication element is missing, resulting in no
password -->
         <savepref>No</savepref>
         <groupid>Management</groupid>
      </user>
      <user>
         <userid>jbird</userid>
         <description>John Bird</description>
         <savepref>No</savepref>
         <groupid>Management</groupid>
      </user>

        <!-- Add Project Leaders with basic passwords -->
      <user>
         <userid>gbaker</userid>
         <description>George Baker</description>
         <authentication type="pw">
            <pw>gwbpassword</pw>
            <changepw>yes</changepw>
         </authentication>
         <groupid>ProjectLeaders</groupid>
         <savepref>Yes</savepref>
      </user>
      <user>
         <userid>drussell</userid>
         <description>David Russell</description>
         <authentication type="pw">
            <pw>drpassword</pw>
            <changepw>yes</changepw>
         </authentication>
         <groupid>ProjectLeaders</groupid>
         <savepref>Yes</savepref>
      </user>
      <user>
         <userid>swatts</userid>
         <description>Steve Watts</description>
         <authentication type="pw">
            <pw>swpassword</pw>
            <changepw>yes</changepw>
         </authentication>
         <groupid>ProjectLeaders</groupid>
         <savepref>Yes</savepref>
      </user>

        <!-- Add Residents with Native Authentication passwords -->
      <user>
```

```
         <userid>bogardus</userid>
         <description>Bob Bogardus</description>
         <authentication type="native">
      <!-- notice changepw is ignored when using native authentication -->
         </authentication>
         <groupid>Residents</groupid>
         <savepref>Yes</savepref>
      </user>
      <user>
         <userid>cohen</userid>
         <description>Alan Cohen</description>
         <authentication type="native">
         </authentication>
         <groupid>Residents</groupid>
         <savepref>Yes</savepref>
      </user>
      <user>
         <userid>agoneal</userid>
         <description>Anna Murphy</description>
         <authentication type="native">
         </authentication>
         <groupid>Residents</groupid>
         <savepref>Yes</savepref>
      </user>
   <!-- Add a session to George Baker -->
      <session>
         <description>HODLinux</description>
         <filename>HODLinux.hod</filename>
         <userid>gbaker</userid>
      </session>

   </action>
</dirscript>
```

Command-line options

Here are some samples of executing Directory Utility using the sample XML file specified in Example 7-5 on page 368:

1. If you are running Directory Utility on an AIX machine with the Host On-Demand server on the same machine using the default port, specify:

   ```
   DirUtil ITSOSample.xml admin password 127.0.0.1
   ```

2. If you are running Directory Utility on a z/OS system with the Host On-Demand server on the same machine using port 8998 for the Service Manager port, specify:

   ```
   DirUtil ITSOSample.xml admin password 127.0.0.1 8998
   ```

3. If you are running Directory Utility on a Windows system running a locally installed client with the Host On-Demand server on another machine, listening on the default port, specify:

```
DirUtil ITSOSample.xml admin password HODLinux.itso.ral.ibm.com
```

7.8 Java 2 considerations for iSeries

If you have configured Host On-Demand to use a V1.4 JVM, you must perform the following to allow the DirUtil script to operate properly:

1. Run **`EDTF '/qibm/proddata/hostondemand/lib/samples'`**
2. Type `5` next to DirUtilCommandFiles.
3. Type `2` next to DirUtil-AS400.sh.
4. Locate the words `Modify the following to specify your java engine`
5. Add `JAVA_ENGINE="java -Djava.version=1.4"`
6. Comment out the other JAVA_ENGINE statement by typing a `#` in the first column of the line.

8

LDAP directory server

In its default configuration, Host On-Demand stores its configuration information in a non-shared private data store. Enterprise customers often need to manage Host On-Demand user and group configuration information for multiple Host On-Demand servers. If these enterprise customers were to use the default non-shared private data store, it would require them to separately manage each instance of Host On-Demand. The deployment and use of an LDAP directory simplifies the administration of multiple Host On-Demand servers using the Configuration Server-based model. In addition, if your intent is to deploy Native Authentication the deployment of LDAP directory is also required. For details about Native Authentication, refer to 11.11, “Native Authentication” on page 453.

This chapter focuses on the following issues relative to the implementation of an LDAP directory server with Host On-Demand:

- LDAP overview
- Supported LDAP directory servers
- Configuring supported LDAP directory servers
- Host On-Demand LDAP directory operations
- Availability, performance, backup and recovery

8.1 LDAP overview

This section provides an introductory overview of LDAP and the benefits it provides for administrators of large network enterprises. Readers who want a broader understanding of the LDAP model than provided here should refer to the following redbooks:

- *Understanding LDAP*, SG24-4986
- *LDAP Implementation Cookbook*, SG24-5110
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*, SG24-6163

The basic unit of information stored in the directory is called an entry. An entry represents objects of interest such as organizations, people, servers, etc. Entries are composed of a collection of attributes that contain information about each object. Every attribute has a type and one or more values. The type of the attribute is associated with a syntax, which specifies what values can be stored. For example, an entry can have a telephone attribute. The syntax associated with this type of attribute specifies that the values are telephone numbers represented as printable strings. It is possible for the directory entry for an organization to have multiple values in this attribute. In addition to defining what data can be stored as the value of an attribute, the syntax of an attribute also defines how those values behave during searches and other directory operations.

Schema files define the types of objects that can be stored in the directory; they also list the attributes of each object type and whether these attributes are required or optional. For example, in the person schema, the attribute *surname* is required, but the attribute *description* is optional. Schema checking ensures that all required attributes for an entry are present before an entry is stored.

Host On-Demand uses a specific schema, called an *ePerson*. This schema is shipped with all current IBM LDAP directory servers; however, if you are using the Netscape directory server or an older release of an IBM LDAP directory server you will need to extend the schema of that directory server to include the ePerson schema. Host On-Demand provides this schema. If required, the schema files must be manually installed on an LDAP server, and must be in effect before Host On-Demand can store configuration information in an LDAP server. Refer to 8.4, “Schema installation” on page 375 for detailed instructions on the installation of the Host On-Demand schema files.

8.2 Host On-Demand and LDAP overview

The default implementation of Host On-Demand uses a private data store model, which does not provide sharing across servers; however, you may optionally use an LDAP directory to store and retrieve configuration information. You may start your Host On-Demand deployment by using the LDAP directory server or you may start using the default private data store, and migrate your configuration information to the LDAP directory server later. You can later revert to using the private data store if for example, you cannot connect to the LDAP directory for any reason; however, you cannot migrate information from an LDAP directory back to a private data store. Specific migration issues are detailed in 8.5.3, “LDAP migration implications” on page 380.”

8.3 Supported LDAP directory servers

Host On-Demand supports the following LDAP directory servers:

- IBM LDAP Directory Server V3.2.2, IBM Directory Server V4.1 & V5.1.

  This directory server is available from the following IBM Internet site:

  http://www.ibm.com/software/network/directory/

- Netscape Directory Server V4.0 (both on Windows and AIX)

  Information on the Netscape Directory Server may be obtained at:

  http://enterprise.netscape.com/products/identsvcs/directory.html

  The schema for all Netscape directory servers must be extended as documented in 8.4, “Schema installation” on page 375.

- IBM LDAP Server running on OS/390 Version 2 Releases 9, and 10

  The schema for this LDAP directory server must be extended for Version 2 Release 9. Beginning with Release 10, the Host On-Demand required schema was shipped in the default schema for the TDBM configuration option. Refer to 3.8, “LDAP directory server” on page 121 for complete details on installing and using the zSeries LDAP directory server.

- IBM LDAP Server running on z/OS V1R1, V1R2, V1R3, and V1R4

8.4 Schema installation

The IBM standard schema is required by Host On-Demand. If you are using an LDAP directory server that does not already support this schema, see 8.3, “Supported LDAP directory servers” on page 375. You must extend the schema. Host On-Demand provides the extensions for these servers in several files that are located in the publish subdirectory of the Host On-Demand installation directory (for example, `C:\Program Files\IBM\HostOnDemand\HOD\ldap`). These files contain extensions to the shipped LDAP schema and are stored in standard slapd format. The schema extensions must be in effect before Host On-Demand can contact, and store configuration information in an LDAP server. If your LDAP administrator has already installed these schema extensions for use by another IBM product, you can skip the following steps; otherwise, follow these steps to install the schema on your directory server.

8.4.1 Netscape Directory Server

Follow these instructions to install the schema on the Netscape Directory Server:

1. Copy the following files from the \HostOnDemand\HOD\ldap directory to the Netscape LDAP config directory on the LDAP server:

   Netscape.IBM.at

   Netscape.IBM.oc

2. Stop the LDAP server.
3. Edit the <Netscape LDAP config directory>`/slapd.conf` file and add the following statements:

   ```
   userat “<Netscape LDAP config directory>/Netscape.IBM.at”
   useroc “<Netscape LDAP config directory>/Netscape.IBM.oc”
   ```

4. Restart the LDAP server.

8.4.2 IBM SecureWay LDAP Directory Server

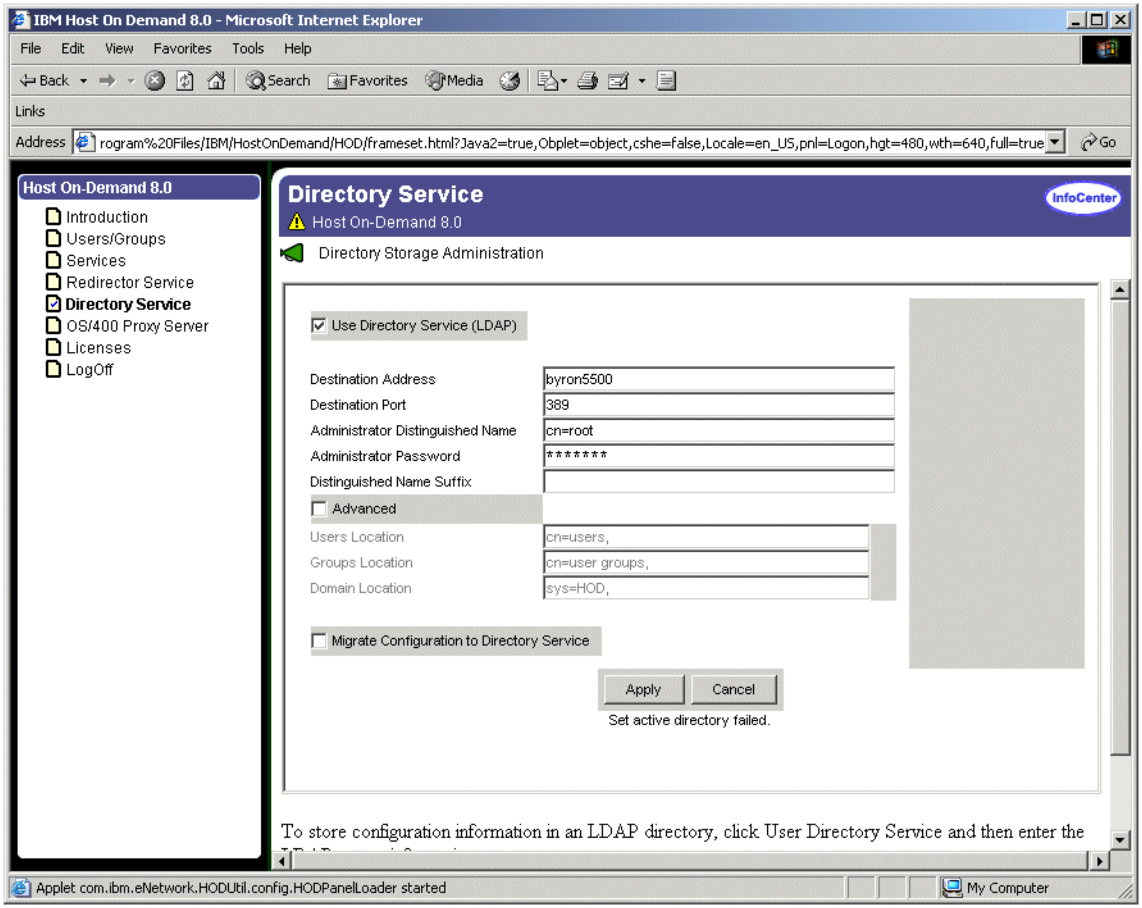
If you are using the IBM LDAP Directory Server on zSeries, you will find your instructions in 3.8.1, “Schema installation” on page 121.

8.5 Host On-Demand directory operations

The default operational mode for Host On-Demand is to use the private data store. Using an LDAP directory server to manage and share your definitions across multiple Host On-Demand servers is an option that must be carefully planned and executed.

8.5.1 Switching to an LDAP directory server

Enabling LDAP directory support is performed by the administrator through the window shown in Figure 8-1. Details on how to complete this window are discussed in 7.4.1, “Use Directory Service (LDAP)” on page 350. This section discusses the process that takes place when you switch from the private data store to an LDAP server, and some common events that may occur when you do.



Address: rogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true

☑ Use Directory Service (LDAP)

Destination Address: byron5500
Destination Port: 389
Administrator Distinguished Name: cn=root
Administrator Password: *******
Distinguished Name Suffix:

☐ Advanced

Users Location: cn=users,
Groups Location: cn=user groups,
Domain Location: sys=HOD,

☐ Migrate Configuration to Directory Service

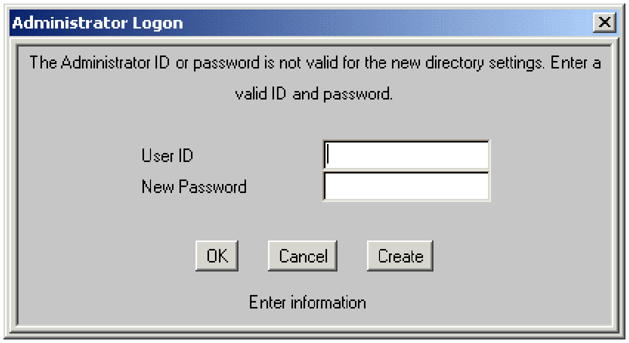
Set active directory failed.

To store configuration information in an LDAP directory, click User Directory Service and then enter the

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 8-1 Enable LDAP directory service

It is important to understand the process of switching to the LDAP directory so that you will realize what is happening if the window shown in Figure 8-2 appears while the switch to the LDAP server is taking place.



Administrator Logon

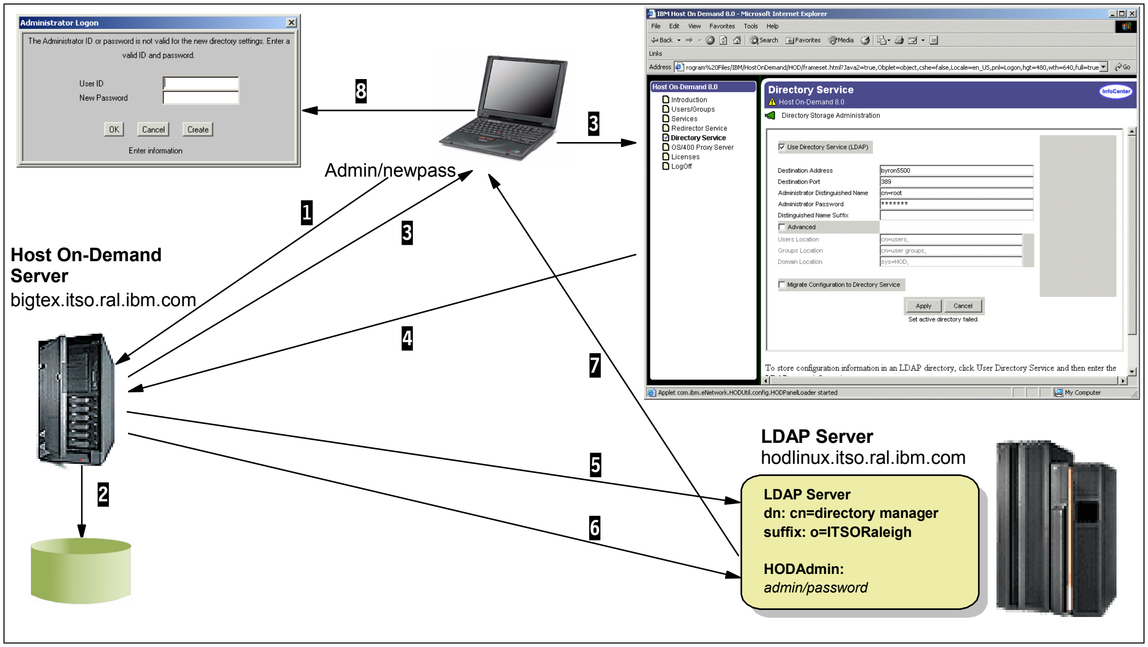
The Administrator ID or password is not valid for the new directory settings. Enter a valid ID and password.

User ID
New Password

Enter information

Figure 8-2 LDAP password failure

To understand what caused the error, you must understand what happens during the switch. Figure 8-3 depicts the process flow when the administrator clicks **Apply** in the window shown in Figure 8-1 to activate the LDAP directory.



Administrator Logon

The Administrator ID or password is not valid for the new directory settings. Enter a valid ID and password.

User ID
New Password

Enter information

IBM Host On Demand 8.0 - Microsoft Internet Explorer

Address rogram%20Files/IBM/HostOnDemand/HOD/frameset.html?Java2=true,Obplet=object,cshe=false,Locale=en_US,pnl=Logon,hgt=480,wth=640,full=true

Directory Service

Host On-Demand 8.0

Directory Storage Administration

☑ Use Directory Service (LDAP)

Destination Address byron5500
Destination Port 389
Administrator Distinguished Name cn=root
Administrator Password *******
Distinguished Name Suffix

□ Advanced

Users Location cn=users,
Groups Location cn=user groups,
Domain Location sys=HOD,

□ Migrate Configuration to Directory Service

Set active directory failed.

To store configuration information in an LDAP directory, click User Directory Service and then enter the

Applet com.ibm.eNetwork.HODUtil.config.HODPanelLoader started

Figure 8-3 Switch to LDAP directory server

Here are the steps:

1. The administrator logs on, using `admin` as the user ID and `newpass` as the password (assume the password has been previously changed).

2. The Host On-Demand Service Manager successfully authenticates the user ID/password (`admin/newpass`) with that contained in the private data store (`admin/newpass`).
3. The administrator enters the required information to switch to the LDAP server.
4. When the administrator clicks **Apply**, the Service Manager contacts the LDAP server, passing the LDAP administrator's distinguished name (DN) (`cn=directory manager`) and password (note that this password is not the password used to log in to HODAdmin.html), and the suffix (`o=ITSORaleigh`), at which point the Host On-Demand information will be inserted into the directory.
5. The LDAP server authenticates the request as follows:

   a. Are the DN and password valid as the LDAP administrator?

   b. Is the suffix defined and initialized?

   If the DN and suffix are validated, the Service Manager can proceed.
6. The Host On-Demand Service Manager attempts to create the default Host On-Demand administrator user ID (`admin`) and password (`password`). If this is the first time this directory has been contacted (or if the `admin` ID does not exist), this update will succeed. If the `admin` ID already exists, the request will fail to create the user ID since it is already present (the existing password need not be `password`); however, the Service Manager ignores the failure and proceeds.
7. This step is similar to step 2. on page 379. The only difference is that this step is performed with the new LDAP settings. The administration applet is now prompted to reauthenticate itself to the LDAP server, and it responds by sending `admin/newpass`. In this example, the authentication fails (the directory service is expecting `admin/password`), which results in the window shown in Figure 8-2. You should enter the user ID and password of an administrative user that are valid for the new LDAP settings (in our example, `admin/password`).

   > **Note:** Remember that multiple Host On-Demand systems can use the same LDAP server and suffix to allow for workload balancing, so another system may have reset this password.

8. After the appropriate user ID/password combination is entered, the user is then authenticated and the Service Manager finishes creating the required information in the LDAP directory.

9. Finally, if the migration checkbox was checked, the information in the private data store is created in the LDAP directory. An audit trail of all updates is maintained in HostOnDemand\private\hodldap.log.

8.5.2 Unable to enable LDAP

If you are using the Netscape LDAP directory and are unable to successfully enable LDAP, you may need to temporarily disable the UID uniqueness filter in the LDAP directory. Each user or person object created in an LDAP directory has a User ID (UID) field. Some of the objects created by Host On-Demand during the initialization process may be rejected by the UID uniqueness filter.

To resolve this problem do the following:

1. Open the Directory Server Console for your Netscape Directory
2. Navigate to the Configuration tab.
3. Expand the plug-ins.
4. Select **uid uniqueness.**
5. Clear the associated checkbox.
6. Click **Save.**
7. Restart the LDAP server.

> **Important:** Do *not* leave UID uniqueness disabled permanently. The UID uniqueness plug-in should be disabled only if you are having trouble enabling LDAP for Host On-Demand. After enabling LDAP, your should re-enable UID uniqueness.

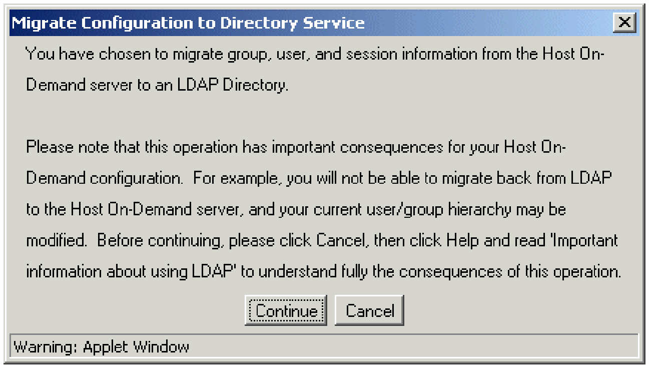
8.5.3 LDAP migration implications

Before converting to the LDAP directory server, make sure that you understand all the issues in this section, because any changes made in the LDAP directory cannot be migrated back to the private data store.

Hierarchical structure

LDAP enables you to manage Host On-Demand configuration information by arranging those users into a hierarchical tree of groups. A group can have one or more subgroups as children, and each subgroup inherits all of the sessions defined by the parent group. A user can be an immediate member of any one group, and inherits sessions from all the groups in its inheritance tree. This means that you can define sessions in a high-level group for a large number of users and subgroups, and then customize them in lower-level groups for a smaller numbers of users. It also means that a user cannot belong to more than one group.

The Host On-Demand private data store is not arranged hierarchically; therefore, migrating your configuration information to an LDAP directory changes the relationship between your users and groups. Specifically, all groups and their sessions become children of the specified suffix in the LDAP directory, and all users become members of one of the groups that they were members of before migration. Users that are members of multiple groups will not lose configuration information as a result of migration, because the group settings will be allocated to them as individual users.



Migrate Configuration to Directory Service

You have chosen to migrate group, user, and session information from the Host On-Demand server to an LDAP Directory.

Please note that this operation has important consequences for your Host On-Demand configuration. For example, you will not be able to migrate back from LDAP to the Host On-Demand server, and your current user/group hierarchy may be modified. Before continuing, please click Cancel, then click Help and read 'Important information about using LDAP' to understand fully the consequences of this operation.

Figure 8-4 Migration warning

Migration process

The migration process assumes that items are taken from the private data store and added to the LDAP directory. Migration is subject to the following rules:

- If a group or user already exists in the LDAP directory, that entry is skipped.
- Groups are migrated before users.
- A user is added to a single group. There is no way of knowing exactly which group a user will be added to; however, it appears to be a function of the order in which the groups are created in the private data store, and the order in which the user is added to a group. The migration log, hodldap.log, provides details about to which group a user is added.
- Sessions that a user would have inherited from groups that the user did not migrate to are not lost. These sessions are assigned at the user level.

During the migration, a progress indicator will be displayed, showing the status of the process (Figure 8-5).

Figure 8-5 Migration progress

Private data store status

After you have migrated your configuration information to the LDAP directory, and as long as you are using the LDAP directory, the users, groups, and sessions that are defined in the private data store will not be accessible to the administrator or a client. The private data store is preserved and is not modified by the migration process, but any changes made in the LDAP directory cannot be migrated back to the private data store.

Reverting to the private data store

You can revert to using the Host On-Demand private data store, but remember that none of the user or group changes made while you were using the LDAP directory will be reflected in the private data store. Follow the instructions below to switch back to the private data store:

1. Log on to Host On-Demand as the administrator.
2. Select **Directory Service** (refer to Figure 8-1 on page 377).
3. Clear the Use Directory Service (LDAP) checkbox.
4. Click **Apply**.

> **Note:** You do not have to restart the Service Manager when switching back to the private data store. If you later want to switch back to the same directory server, you can do so without restarting the Service Manager. However, if you switch to a different directory, follow the instructions in the next section.

Switching to a Different LDAP directory server

If you are using an LDAP directory as a data store, and it becomes necessary to switch to another LDAP server, you must perform the following steps carefully:

1. Revert to the private data store; refer to “Reverting to the private data store” on page 382 for instructions.
2. Restart the Service Manager.
3. Log on as the administrator and enter the address information for the new LDAP server (refer to 7.4.1, “Use Directory Service (LDAP)” on page 350).
4. Activate the new LDAP directory server.

Multiple Host On-Demand system implementation

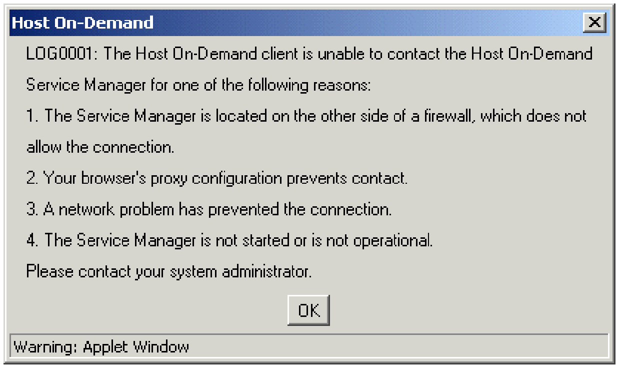
It is recommended that you create a separate administrator ID to be used for LDAP on all your Host On-Demand servers. Use this ID to do your administration, and leave the defaults (`admin/password`) alone. The advantage of this is that regardless of which Host On-Demand server switches or migrates data to the LDAP server, the password for the administrative ID used to do the switch will not be compromised.

8.6 Operational issues

This section covers some operational issues for the administrator.

8.6.1 Startup sequence

When the Service Manager starts, it reads the data store to get its configuration information. When Host On-Demand is using the private data store, this works very smoothly; however, when Host On-Demand is configured to use an LDAP directory, a dependency on the directory server is introduced. The directory server must be operational prior to the startup of the Service Manager so that it can read the data store from the directory server. If the LDAP directory server is not operational, the Service Manager will periodically retry the connection until it is successful. Until the Service Manager connects with the LDAP directory server, it will not accept any end user or administrative client connections. The symptom the user will see is a LOG0001 error message as shown in Figure 8-6.



LOG0001: The Host On-Demand client is unable to contact the Host On-Demand Service Manager for one of the following reasons:

1. The Service Manager is located on the other side of a firewall, which does not allow the connection.
2. Your browser's proxy configuration prevents contact.
3. A network problem has prevented the connection.
4. The Service Manager is not started or is not operational.

Please contact your system administrator.

Figure 8-6 LOG0001 error

8.6.2 Reverting to the private data store if a directory server fails

If you must get your Host On-Demand server operational after an LDAP directory server failure, you can revert to the Host On-Demand Private data store. However, doing so means that you will not have access to any additions made to the LDAP directory server since you migrated from the private data store.

Because your Host On-Demand server is configured for LDAP directory server use, you must clear this condition and restart the Service Manager. To clear the condition, delete the `dirInfo.active` file in the `\HostOnDemand\private` directory, then restart the Service Manager. This clears the configuration of references to the directory server so that when the Service Manager starts, it will be using the private data store. After the LDAP directory server is again operational, you can follow the procedure in 7.4.1, “Use Directory Service (LDAP)” on page 350 to re-enable the LDAP directory support.

8.6.3 Debug tracing of the Service Manager

There is a special trace facility for debugging problems with the Host On-Demand Service Manager. To enable this, add one of the following flags to the end of the command line that is used to start the Service Manager: /d, /d1, /d2, or /d3.

The /d flag turns on tracing. The /dn flag (where n is 1, 2 or 3) sets the debug level. Level 1 produces very little trace information; levels 2 and 3 produce progressively more information.

On Windows NT the Service Manager runs as a system service, so to use this trace facility, we recommend you stop the service and run the Service Manager from a command prompt. Example 8-1 shows a sample command file; modify it for your own installation.

Example 8-1 Sample debug command file

```
set PATH=%PATH%;c:\Program Files\IBM\HostOnDemand\bin

c:\Program Files\IBM\HostOnDemand\bin\jre.exe -mx20000000 -nojit -classpath
c:\Program
Files\IBM\HostOnDemand\lib\rt.jar;c:\hostondemand\lib\i18n.jar;c:\Program
Files\IBM\HostOnDemand\lib\ibmjndi.jar;c:\Program
Files\IBM\HostOnDemand\lib\jndi.jar;c:\Program
Files\IBM\HostOnDemand\lib\jsdk.jar;c:\Program
Files\IBM\HostOnDemand\lib;c:\Program
Files\IBM\HostOnDemand\lib\ods.jar;c:\Program Files\IBM\HostOnDemand\lib\sm.zip
com.ibm.eNetwork.HODUtil.services.admin.NCServiceManager c:\Program
Files\IBM\HostOnDemand /d3 > output.log
```

On OS/390, the `ServiceManager.sh` shell script found in the `/hostondemand/lib` directory has a Java command statement commented out for the /d3 tracing. Uncomment the statement that has the /d3 trace and the output redirected into `/private/HOD.stdout`. Restart the Service Manager.

8.6.4 LDAP logs

Several logs are maintained by the Service Manager, some of which are present only if you use the LDAP directory server for the data store.

The `\HostOnDemand\private\server.log` contains LDAP operational messages for the current execution of the Service Manager. This file is overwritten every time the Service Manager starts the LDAP interface.

The `\hostondemnd\private\hodldap.log` is introduced with the LDAP directory server. This file contains an audit trail of the migration from the private data store to the LDAP directory data store. It is especially useful when you migrate users that exist in multiple groups to an LDAP directory, because a user can only belong to a single group in the directory server data store. This log tells you into which group a specific user is migrated, if it belonged to multiple groups in the private data store.

There are three subdirectories that are used, or created if they do not exist, when the LDAP interface is activated. Below is an explanation of what you will find in these logs:

- The \HostOnDemand\private\Tivolilogs\ subdirectory contains three trace files, trace1.log, trace2.log and trace3.log, which track activity information on updates to the directory server. These three files are used in a round-robin fashion whenever the Service Manager starts (that is, trace1 is used, then trace2 the next time, then trace3, then trace1 again).
- The \HostOnDemand\private\serverlogs\ subdirectory contains a round-robin set of files that contain Java error messages relating to LDAP operations.
- The \HostOnDemand\private\OpMgr\ subdirectory contains three logs: UEvents1.log, UEvents2.log, and UEvents3.log, used in a round-robin fashion, which contain Java events regarding the LDAP operations.

9

Configuration servlet

The traditional technique for retrieving and saving user preferences is for the Host On-Demand client to talk directly to the Host On-Demand configuration server through a predefined port, 8999 by default. Although efficient, this method has two drawbacks when used in an environment that demands security:

- It requires that the port be opened through a firewall.
- The data between the client and the Configuration Server is not encrypted.

This chapter discusses the configuration servlet feature of Host On-Demand and how it can be used to address these drawbacks.

9.1 Overview

Host On-Demand client configuration information and applet code is downloaded from the Host On-Demand server to the client. The Host On-Demand Service Manager running on a Web server communicates with the clients to download all the required applet code, configuration information, session information, and so on. By default, the Host On-Demand Service Manager is set up to listen on a single port (8999 by default, but it can be modified during installation). All Host On-Demand applets communicate with the Service Manager by opening a Java socket to this port on the server. Refer to Figure 9-1.

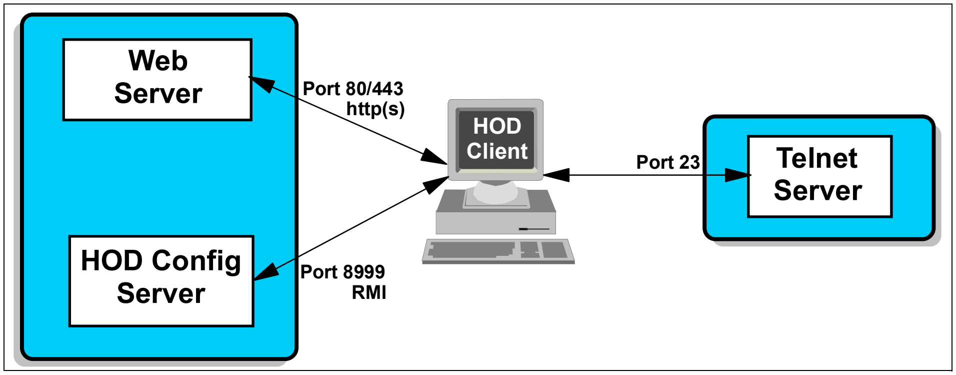


Figure 9-1 Host On-Demand default configuration flow

The initial request from a browser to the Host On-Demand server is over port 80 (or port 443 is using SSL). The Host On-Demand client applets, configuration information, user, group, and session information are downloaded to the client from the Host On-Demand Service Manager over port 8999.

However, this requires that port 8999 must be opened on the server machine and any firewalls that may be between the server and the client. In addition, the data transfer between the client and the Configuration Server is not encrypted.

To resolve these issues, the configuration servlet can be used to tunnel the configuration information between the client and the servlet over an HTTP(S) connection, and then to pass that information on to the Host On-Demand configuration server of choice over the defined configuration port. This resolves both of the above-mentioned issues by using the existing HTTP(S) port already open through the firewall, and the encryption of the data by using HTTPS.

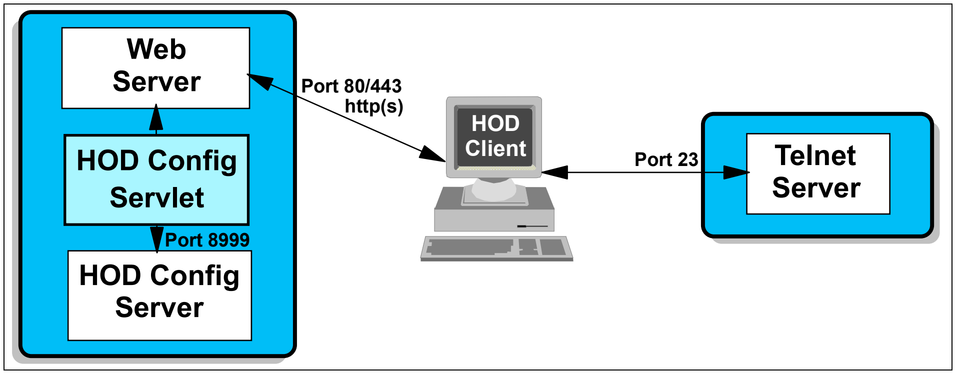


Figure 9-2 Host On-Demand configuration flow with configuration servlet

The implementation of the configuration servlet requires a Web server that supports servlets, such as WebSphere Application Server, Lotus Domino, or iPlanet Web Server. There are many products that are capable of running the configuration servlet, and the configuration procedure for each is different. Check your Web server and servlet engine documentation for servlet configuration details on your operating system.

9.2 Installation

During Host On-Demand installation, you can choose to have the configuration servlet installed and configured on OS/400, Windows, AIX, Linux, Solaris, and HP-UX for IBM WebSphere Application Server Version 4.0 and 5.0.

The following Web application servers are supported in IBM WebSphere Host On-Demand V8:

- IBM WebSphere Application Server Version 4.0, 5.0, and 5.0 Express
- Lotus Domino R6
- iPlanet Application Server V6.0

For more detailed information on installing the configuration servlet on various platforms, see “Chapter 7” in *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301, (or the online version of *Planning, Installing, and Configuring Host On-Demand* installed with HOD).

> **Note:** You must manually install the Host On-Demand configuration servlet in any environment where the servlet is not automatically installed and configured, or when the servlet is to be added after Host On-Demand is installed.

9.2.1 Manual installation

When you are manually installing the configuration servlet, you should use cfgservlet.EAR file located under <hod_root>/lib/ directory. For information on how to deploy the EAR file, please refer to documents on Web application servers you are using.

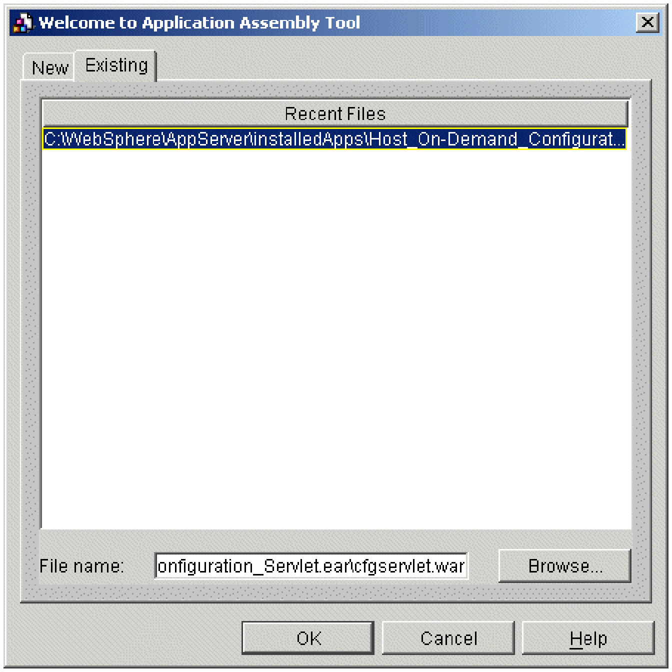
Tip: For WebSphere Application Server 5: After you save your deployment settings in the administrative console, you need to start the Host On-Demand configuration servlet in the Enterprise Applications window of WebSphere Application Server. Then go to the Environment window and select **Update Web Server Plug-in**.

9.3 Modifying configuration servlet

IBM WebSphere Host On-Demand automatically configures WebSphere Application Server 4.0 and 5.0.

9.3.1 Accessing Configuration Servlet

Use the Application Assembly Tool (AAT) that is installed with WebSphere Application Server to modify the default servlet configuration. Start the Application Assembly Tool, and choose to edit an existing application as shown in Figure 9-3.

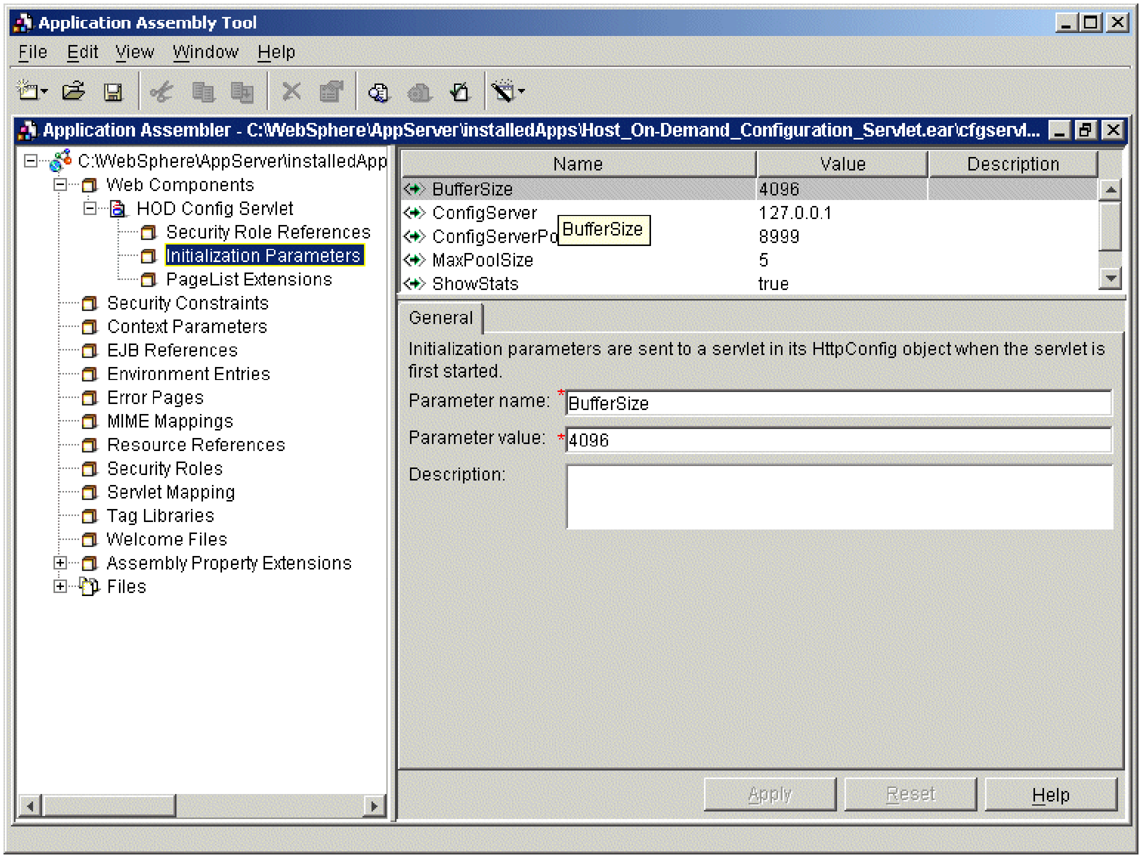


C:\WebSphere\AppServer\installedApps\Host_On-Demand_Configurat...

File name: onfiguration_Servlet.ear\cfgservlet.war

Figure 9-3 Modifying HODConfig Servlet with WAS 4.0

Now it is a simple process to choose the parameters associated with HODConfig.



Name	Value	Description
BufferSize	4096	
ConfigServer	127.0.0.1	
ConfigServerPo	8999	
MaxPoolSize	5	
ShowStats	true	

Initialization parameters are sent to a servlet in its HttpConfig object when the servlet is first started.

Parameter name: * BufferSize

Parameter value: * 4096

Description:

Figure 9-4 HODConfig Parameters with WAS 4.0

9.3.2 Testing the servlet

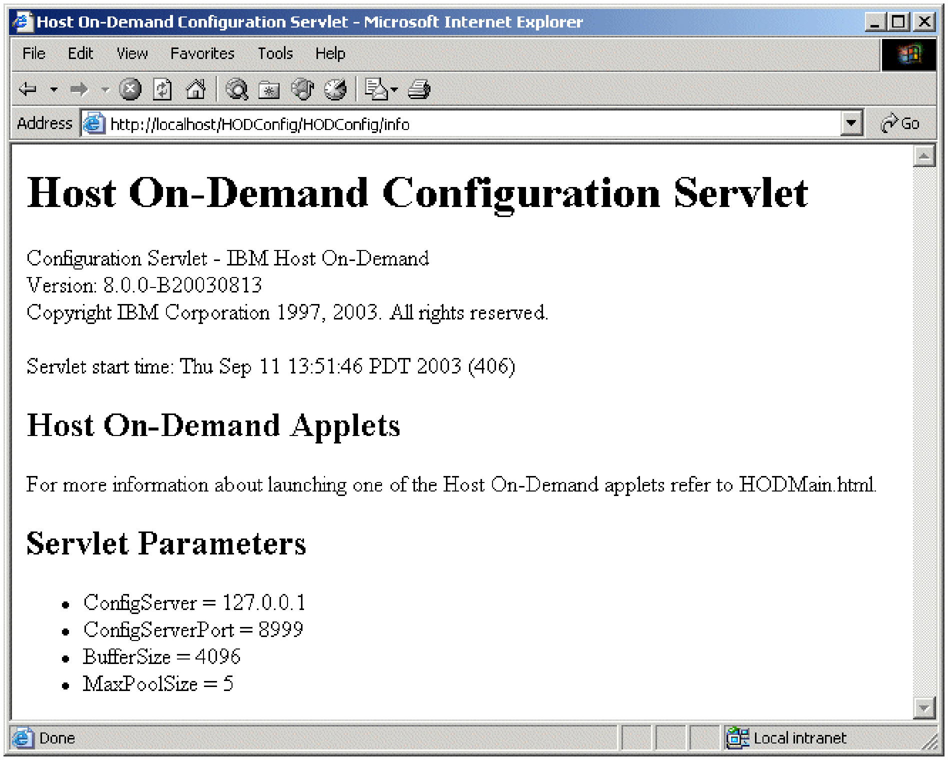
After installing a configuration servlet to your machine, it is recommended that you test the servlet by invoking the ShowStats function. This is done by specifying the following URL from a browser:

```
http://server_name/servlet_location/HODConfig/info
```

Using the example just created, the URL should look like the following:

```
http://server_name/HODConfig/HODConfig/info
```

When successful, your browser will return a window similar to that shown in Figure 9-5.



Host On-Demand Configuration Servlet - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost/HODConfig/HODConfig/info
Go
Done
Local intranet

Host On-Demand Configuration Servlet

Configuration Servlet - IBM Host On-Demand
Version: 8.0.0-B20030813
Copyright IBM Corporation 1997, 2003. All rights reserved.

Servlet start time: Thu Sep 11 13:51:46 PDT 2003 (406)

Host On-Demand Applets

For more information about launching one of the Host On-Demand applets refer to HODMain.html.

Servlet Parameters

- ConfigServer = 127.0.0.1
- ConfigServerPort = 8999
- BufferSize = 4096
- MaxPoolSize = 5

Figure 9-5 Servlet information

9.4 Enabling clients

There are two ways to enable a client to use the configuration servlet:

- Set the ConfigServerURL parameter in the config.properties file, which is located under HostOnDemand/HOD/ directory. When this parameter is detected in the config.properties file, all clients will use this method of communication with the Host On-Demand configuration server.
- Use Deployment Wizard to configure HTML for the configuration servlet model.

Note: IBM recommends that you use the Deployment Wizard to set the ConfigServletURL parameter in the client HTML to `HODConfig/HODConfig/hod`.

9.5 Referencing the configuration servlet

There are two ways to reference the configuration servlet: the direct reference and the indirect reference.

9.5.1 Direct reference

The direct reference is a complete URL. It includes the protocol, HTTP, or HTTPS. For example, if you specify:

```
https://hodserver.raleigh.ibm.com/HODConfig/HODConfig/hod
```

You force the applet to use an encrypted HTTP connection to contact the Host On-Demand configuration servlet running on hodserver.raleigh.ibm.com over the default port 443. If this reference is used, the configuration servlet information will flow over an encrypted session even if the URL used to load the Host On-Demand client specified an unencrypted session, for example:

```
http://hodserver.raleigh.ibm.com/hod/HOD.html
```

This technique may also be used to force the login to a machine other than the one used to load the client. Refer to 9.6, “Implementation scenarios” on page 395 for an example of how this may be used.

9.5.2 Indirect reference

An indirect reference specifies only a path name on the server that launched the Host On-Demand client. Using this method results in the ConfigServerURL being appended to the host portion of the Host On-Demand applet’s URL. For example, if the configuration servlet reference is:

```
/HODConfig/HODConfig/hod
```

and the Host On-Demand applet is loaded using the following URL:

```
https://hodserver/hod/HOD.html
```

then the resulting URL used to contact the configuration servlet is:

```
https://hodserver/HODConfig/HODConfig/hod
```

This method is more flexible, allowing the reference to be used for HTTP and HTTPS connections from a single specification.

9.6 Implementation scenarios

In addition to the obvious use with firewalls, the configuration servlet opens other new ways to deploy Host On-Demand and solve some very difficult issues. We will explore only two: load balancing and Native Authentication.

9.6.1 Load balancing

Let us assume that a company wants to deploy Host On-Demand using a redundant, highly available solution, and also wishes to use the registered user model. In prior releases only one option was available for them: to implement an LDAP directory server to house all user IDs and preferences for all servers, thus providing centralized management. By using the configuration servlet, an additional option becomes available: deploy the configuration servlet and route all login requests to a central system, such as the zSeries, and maintain the information in the Host On-Demand native data store.

In this example the customer has two or more Web servers configured in a redundant load balancing configuration, or two or more servers in physically separate locations providing alternate access points. In either case, the servers are configured identically with the following components:

- A Web server
- A Host On-Demand server
- A configuration servlet running on a Web server that support servlets, Lotus Domino Go Webserver, WebSphere Application Server, or some other Web application server. The servlet is configured to route all requests to a centralized third server. See Figure 9-5 on page 393.

The distributed Host On-Demand systems are configured to accept client login requests. Instead they deploy the configuration servlet, which routes the login requests to the OS/390-based Host On-Demand system, or some other system that processes user login requests. The advantage of this scenario is that all the distributed Host On-Demand servers can be exact clones of one another, and an LDAP directory server is not be required, while still allowing all login processing to be centralized. The remote Host On-Demand servers are optimized for Web serving exclusively, and any platform or combination of platforms, can be used.

9.6.2 Native Authentication

Let us assume the same scenario as described above, but now add the requirement that all users must use their RACF user ID and password. The only modification to the previous scenario is to deploy Native Authentication on the zSeries system, refer to 3.9, “Native Authentication” on page 123. Also refer to 11.11, “Native Authentication” on page 453 for details on how to configure that system. The result is that regardless of the platforms chosen to deploy distributed Host On-Demand servers, all users logging in do so on the same system.

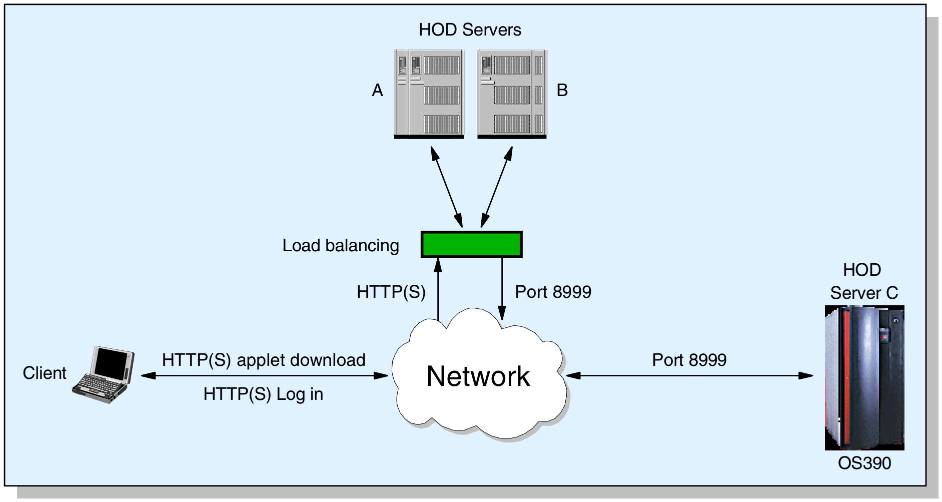


Figure 9-6 Servlet with Native Authentication

9.7 Problem determination

You can access trace, configuration, and statistic information from the configuration servlet for debugging purposes. To access trace information, you need to set the trace parameter to `true` for the configuration servlet. To view the trace, load the following URL into your browser:

```
http://server_name/servlet_alias/HODConfig/trace
```

The configuration servlet’s trace information will be displayed in the browser and written to the servlet engine’s log file.

To access configuration and statistical information, you need to set the ShowStats parameter to `true` for the configuration servlet. To view the information, load the following URL into your browser:

```
http://server_name/servlet_location/HODConfig/info
```

10

OS/400 Proxy

If you are planning to provide file transfer or Database On-Demand to your iSeries (AS/400) users, you may wish to consider using the OS/400 Proxy feature. This feature is only appropriate for connections to an AS/400. It is called a “proxy” because connections are made from the workstation to the O/S400 Proxy Server, which in turn connects to the target iSeries system. The connection will be completed only if the user enters a valid user ID and password on the target iSeries system.

If you will be accessing multiple iSeries systems from the Internet, you may use the OS/400 Proxy to reduce the number of Internet addresses for each target system. If used in conjunction with the Redirector feature, only one address needs to be Internet addressable for multiple back-end systems. In addition, only one port needs to be opened on the firewall (typically port 3470) for the file transfer and Database On-Demand features. The typical ports for file transfer (like ports 20 and 21) can be blocked on the firewall to prohibit direct access.

You may optionally encrypt the connection from the proxy to the back-end host system.

In this chapter, we discuss:

- How to configure a simple session
- Enabling SSL
- How to use the proxy with Database On-Demand
- Sample firewall rules

10.1 How to configure a simple session

In our sample configuration (see Figure 10-1), we are using server C as the Host On-Demand server, the Redirector, and the O/S400 Proxy Server. In practice, each of the services can be split among multiple computers.

One other key concept is that the O/S400 Proxy Server (C) does not necessarily have to be an iSeries. In the example below, we used a Windows 2000 server.

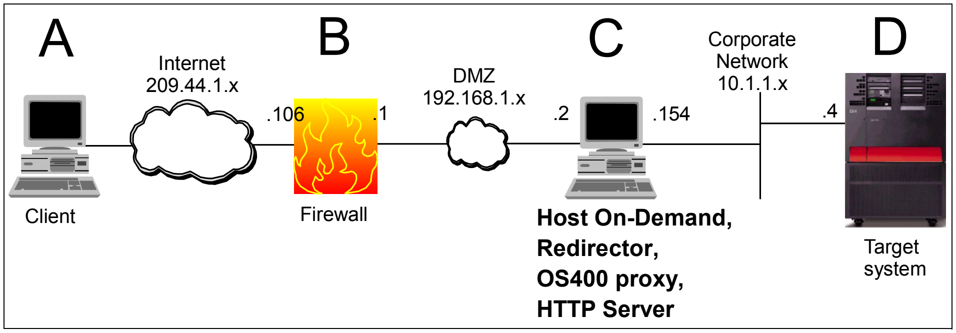


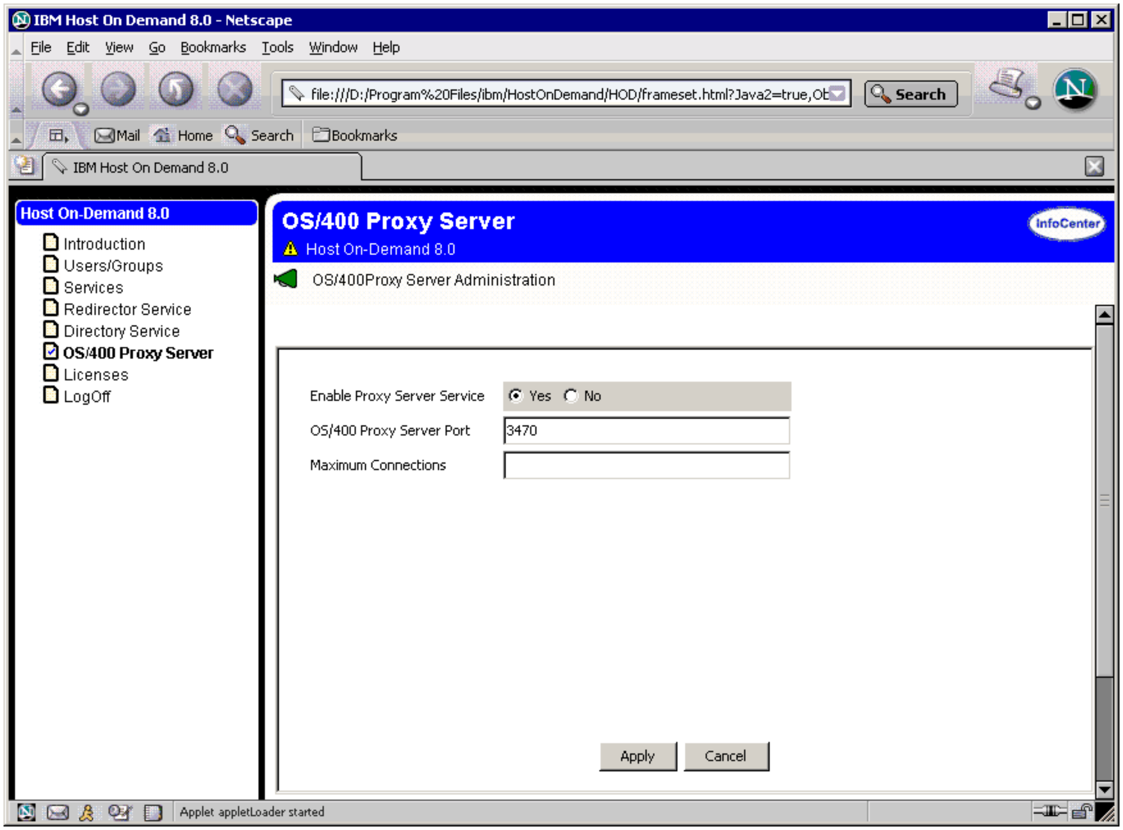
Figure 10-1 Our sample OS/400 Proxy network

The firewall will typically be configured to map a network address using Network Address Translation (NAT).

Table 10-1 Sample NAT rule

System	Internet address	Local address
HOD server	209.44.1.106	192.168.1.2

Figure 10-2 illustrates how you may select the port you wish to use for the proxy server.



IBM Host On Demand 8.0 - Netscape
File Edit View Go Bookmarks Tools Window Help
file:///D:/Program%20Files/ibm/HostOnDemand/HOD/frameset.html?Java2=true,Ot
Search
Mail Home Search Bookmarks
IBM Host On Demand 8.0
Host On-Demand 8.0
Introduction
Users/Groups
Services
Redirector Service
Directory Service
OS/400 Proxy Server
Licenses
LogOff
InfoCenter
Apply
Cancel

OS/400 Proxy Server

Host On-Demand 8.0

OS/400Proxy Server Administration

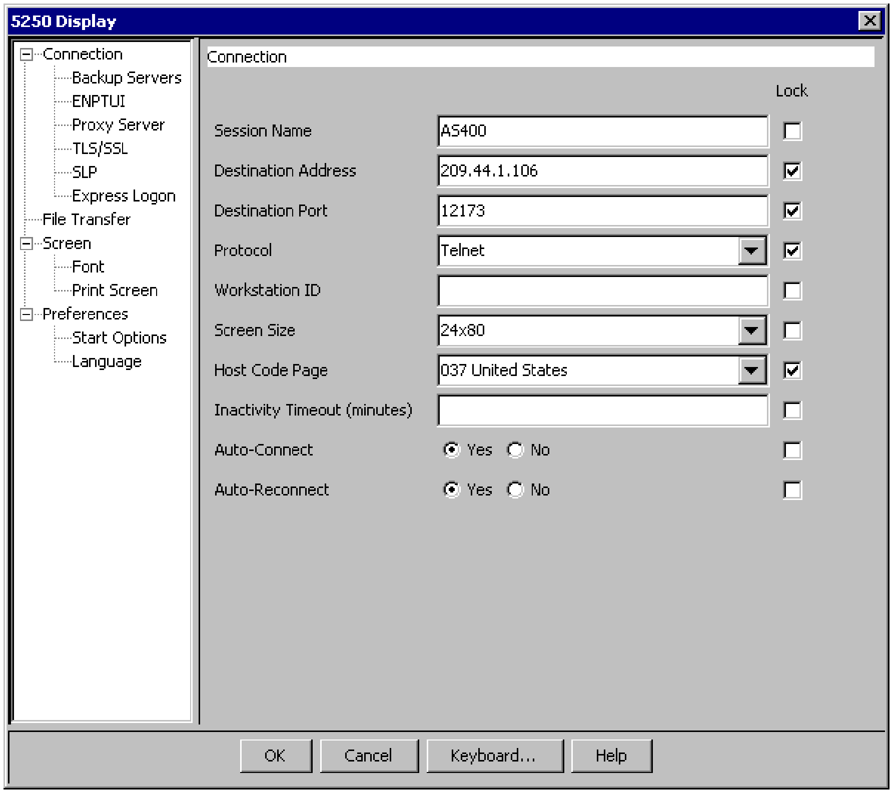
Enable Proxy Server Service	● Yes ○ No
OS/400 Proxy Server Port	3470
Maximum Connections	

Applet appletLoader started

Figure 10-2 O/S400 Proxy Server window within HODAdmin.html

Note: The OS/400 Proxy does not support Telnet connections, and the Redirector does not support non-Telnet connections. Thus, they are typically used together.

Figure 10-3 illustrates a sample redirected session. The session uses the Redirector (C in Figure 10-1) to get to the target iSeries (D).

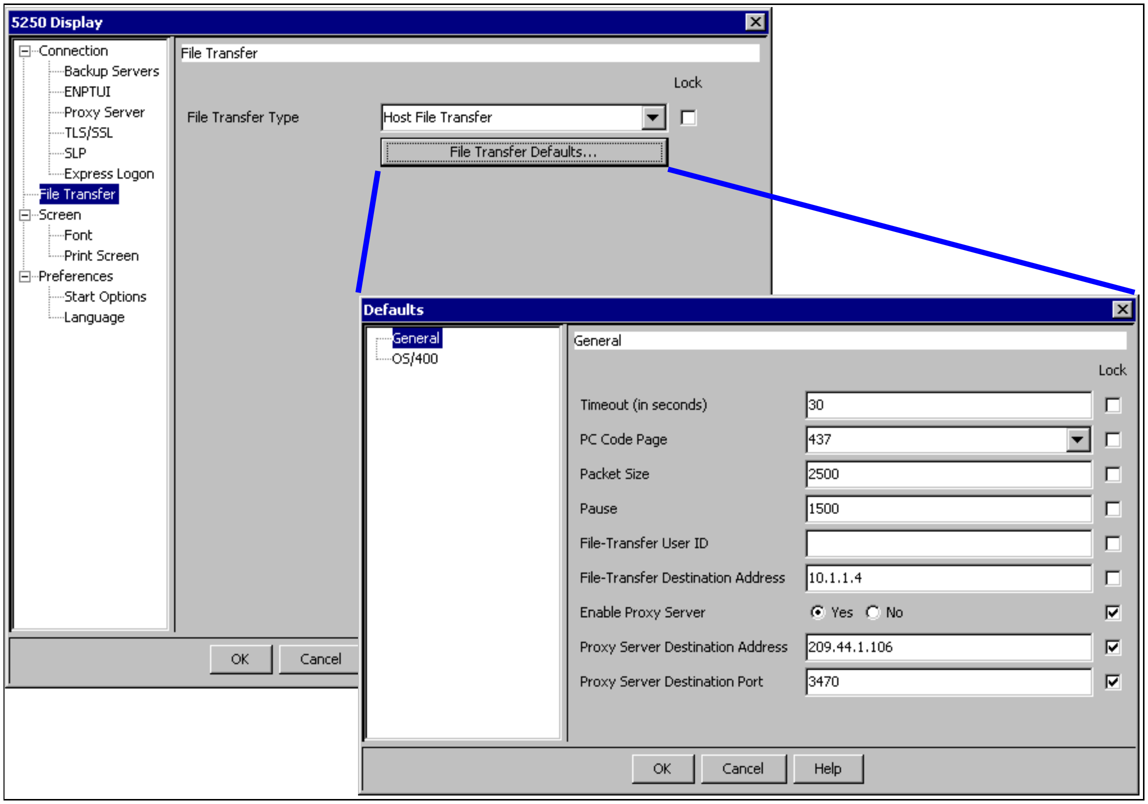


Connection

		Lock
Session Name	AS400	□
Destination Address	209.44.1.106	☑
Destination Port	12173	☑
Protocol	Telnet	☑
Workstation ID		□
Screen Size	24x80	□
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)		□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 10-3 Sample session using Redirector and OS/400 Proxy

Select **File Transfer** from the selection tree in the left pane of Figure 10-3. Then select **File Transfer Defaults**. The windows shown in Figure 10-4 are displayed.



File Transfer Type: Host File Transfer □

		Lock
Timeout (in seconds)	30	□
PC Code Page	437	□
Packet Size	2500	□
Pause	1500	□
File-Transfer User ID		□
File-Transfer Destination Address	10.1.1.4	□
Enable Proxy Server	● Yes ○ No	☑
Proxy Server Destination Address	209.44.1.106	☑
Proxy Server Destination Port	3470	☑

Figure 10-4 File Transfer defaults for the session

Click **Yes** for Enable Proxy Server.

> **Important:** The File Transfer Destination Address field (see Figure 10-4) is resolved by the O/S400 Proxy Server (C in Figure 10-1). If you leave it blank, it will default to the same value as the Telnet session. Since we are using the Redirector, specify the address (or URL) of the target iSeries (D). Also specify the address (or URL) of the target iSeries (D). The O/S400 Proxy Server (C) will need to have access to the corporate DNS, or to have the addresses in its local hosts table.

This concludes the configuration portion. Let us see what the connection looks like in action.

10.2 Using the OS/400 Proxy

There are two components that can utilize the OS/400 Proxy:

- The 5250 file transfer
- Database On-Demand

10.3 Enabling SSL

The following section shows how to make the connection between the proxy and the iSeries system secure.

10.3.1 Prerequisites

The following is required on each target iSeries and iSeries system:

- OS/400 V4R4, or later
- OS/400 Host Servers (5722-SS1 or 5769-SS1, option 12)
- Digital Certificate Manager (5722-SS1 or 5769-SS1, option 34)
- A Cryptographic Access Provider product. You can choose from the following licensed products: 5769-AC1 (40-bit), 5722-AC2 or 5769-AC2 (56-bit), 5722-AC3 or 5769-AC3 (128-bit). The bit size for these products indicates the varying sizes of the digital keys that they employ. A higher bit size results in a more secure connection. Some of these products are not available in all areas due to government export regulations.
- Client Encryption. You may choose from one or more of the following licensed products: 5769-CE1 (40-bit), 5722-CE2 or 5769-CE2 (56-bit), 5722-CE3 or 5769-CE3 (128-bit).

Note: To help you to meet the SSL legal responsibilities, you must change the authority of the directory that contains the SSL files to control user access to the files. In order to change the authority, you must follow the steps below:

1. Enter the command: `wrklnk '/QIBM/ProdData/HTTP/Public/jt400/*'`
2. Select option **9** in the directory (SSL40, SSL56, or SSL128)
3. Ensure *PUBLIC has *EXCLUDE authority.
4. Give users who need access to the SSL files *RX authority to the directory. You can authorize individual users or groups of users.

10.3.2 Configure each target iSeries

The following steps are required on each target iSeries (AS/400) system:

1. From a Web browser enter `http://<server.name>:2001` (where <server.name> is the host name of your iSeries). If you are unable to connect, start the HTTP server with the following OS/400 command:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. Enter a iSeries user profile and password (when prompted). You must have *ALLOBJ authority to complete the configuration activities below.
3. Click **Digital Certificate Manager.**
4. Click **System Certificates.**
5. Click **Work with Secure Applications.**
6. Click **QIBM_OS400_QZBS_SVR_CENTRAL**, then click **Work with System Certificate.**
7. Verify that the *DFTSVR certificate is selected and click **Assign New Certificate**.
8. Repeat steps 6 and 7 for the following applications:
   - QIBM_OS400_QZBS_SVR_DATABASE
   - QIBM_OS400_QZBS_SVR_DTAQ
   - QIBM_OS400_QZBS_SVR_NETPRT
   - QIBM_OS400_QZBS_SVR_RMTCMD
   - QIBM_OS400_QZBS_SVR_SIGNON
   - QIBM_OS400_QZBS_SVR_FILE
   - QIBM_OS400_QRW_SVR_DDM_DRDA

10.3.3 Configuring the OS/400 Proxy keyring

The following instructions are required only on the Host On-Demand server:

1. Type the following OS/400 command:

   ```
   QSH
   ```

2. Type the following command (note `cd` must be in lower case):

   ```
   cd /qibm/proddata/hostondemand/lib
   ```

3. Check to see if some directories exist (if they do not exist, they will be created; if they already exist, you will get a message):

   ```
      mkdir com/ibm/as400
   ```

4. Check for an additional directory:

   ```
   mkdir com/ibm/as400/access
   ```

5. The following command obtains a certificate from the SSL-enabled sign-on server (**Note**: <server.name> is the host name of your iSeries.) Port 9476 is the commonly used port for the “Sign-on” Host Server. This command is in actuality a single line:

   ```
   java -classpath .:/QIBM/ProdData/hostondemand/lib/sm.zip
   com.ibm.hodsslight.tools.keyrng com.ibm.as400.access.KeyRing connect
   <server.name>:9476
   ```

   Restriction: You must enter `toolbox` as the password (*in lowercase*).

6. Multiple pages of information may be displayed; click the **Page-up** and **Page-down** keys to see additional details about the certificates, including the fingerprint. You will typically have two selections to choose from:

   – 0 = Use the Server Certificate
   – 1 = Use the Certificate Authority (CA)

   Always select **0** to trust the server certificate, then press Enter.

7. Repeat steps 1-6 for each target iSeries server.
8. Perform the final step:

   ```
   cp com/ibm/as400/access/KeyRing.class ../hod/com/ibm/as400/access
   ```

10.4 Firewall rules for OS/400 Proxy

Table 10-2 identifies the firewall ports that must be opened if the OS/400 Proxy is used. The key point is that OS/400 Proxy does not negate the need for HTTP and Telnet services.

Table 10-2 Firewall rules for Host On-Demand with OS/400 Proxy

Host On-Demand Function	Firewall ports used	Secure Firewall Ports used
3270 and 5250 Display and Printer Emulation	23 (Telnet) 80 (HTTP)	992 (Telnet) 443 (HTTPS)
File transfer, Database On-Demand	3470 (Proxy Tunnel)	3471 (Proxy Tunnel)
Host On-Demand Administration	80 (HTTP) 8999 (config server)[1]	443 (HTTPS)
License Use Count License Use Management (LUM)	80 (HTTP) 8999 (config server)[2]	

[1] If used in conjunction with the WebSphere configuration servlet, port 8999 is not required. Refer to Chapter 9, “Configuration servlet” on page 387.

[2] To disable License Use Management, refer to 7.6.3, “Disabling License-Use Count” on page 357.

11

Security

Host On-Demand is primarily a downloaded application that obtains the session configuration information from the Web server. This configuration information consists of an IP address and port to access the host system. If you are using a registered user model, you must also have a user ID, and optionally a password that will be used to obtain the configuration information from the server. If you are using an anonymous user model, this information is provided as part of the HTML download process. Finally, host systems also require a user ID and a password to log on.

Unless your Web server is configured for SSL (HTTPS), the login and the transfer of the HTML data is not encrypted, and can be read by a third party. If your users are accessing Host On-Demand and host data from within your intranet, this default security setup might be enough.

If you have users on the Internet accessing Host On-Demand and data on your intranet, you may want additional security. You can configure your Web server to use HTTPS so that the data sent to your browser is encrypted. See your Web server documentation for more information about configuring for HTTPS.

Once the client is loaded in a browser, it communicates directly with the host. The configuration information the configuration server sends to the client regarding the sessions, such as IP address, port number, and user preferences, are not encrypted, unless you have implemented the configuration servlet and utilize HTTPS.

If the Telnet server supports SSL, the clients can be configured to use SSL also. See your Telnet server's documentation for more information about configuring SSL on the Telnet server, and see the Host On-Demand online help for more information about configuring a client to connect to a secure Telnet server.

Using Secure Sockets Layer (SSL) with Host On-Demand extends secure host data access across intranets, extranets, and the Internet. Mobile workers can access a secure Web site, receive authentication, and establish communication with a secure enterprise host. With client and server certificate support, Host On-Demand can present a digital certificate (X.509, Version 3) to the Telnet server, such as IBM Communications Server for Windows NT Version 6, Communications Server for AIX Version 6, OS/400 V4R4 and higher; or IBM Communications Server for OS/390 Version 2.6 or later for authentication.

Host On-Demand can also integrate the SSL client authentication with IBM Vault Registry, providing you with the benefit of using industry-standard public key infrastructure (PKI) methods.

If your Telnet server does not support SSL, and you are running Host On-Demand on Windows NT, Windows 2000 or AIX, you can configure the Host On-Demand Redirector to provide SSL support. The Redirector acts as a transparent proxy between the client and the Telnet server by using port remapping. It can encrypt data between the client and itself, between itself and the host, or both. Refer to the online documentation for instructions on how to configure the Redirector or 7.3.1, “Configuring the Redirector” on page 340.

Starting with Version 8, Host On-Demand also supports the Secure Shell (SSH) for VT and File Transfer (sftp) sessions. Refer to 11.5, “Host On-Demand SSH support” on page 433 for an in depth explanation of SSH, and “VT Display session” on page 309 for information how to set up a session with SSH.

11.1 Signed applet support

The original Java security model prevented a Java applet from:

- Communicating with servers other than the one from which it had originated
- Accessing system resources such as hard disks, printers, and the clipboard

These constraints are often referred to as the sandbox. Their purpose is to:

- Prevent an applet from causing harm on the Internet, which is possible if it were allowed to connect to any destination
- Prevent an applet from doing harm to the machine to which it was downloaded

This was found to be too restrictive in practice, and Java Development Kit (JDK) Version 1.1 introduced the notion of a signed or trusted applet. Such an applet has an embedded X.509 certificate, which identifies the creator of the applet. A user can instruct the browser to allow certain signed applets to operate outside of the sandbox.

To sign an applet, the developer must first obtain a certificate from a Certificate Authority (CA). He can then sign his applet with a special signing tool, which embeds the certificate in the file that contains the applet code. There will usually be two of these: a JAR file for use by Netscape and a CAB file for use by Internet Explorer.

Browsers are preconfigured with public-key certificates from well-known CAs such as VeriSign. When a browser encounters a signed applet from a new source, it checks the embedded certificate to see if it has been signed by one of its preconfigured CAs. If it has, the browser tells the user who the developer is, and asks if the user trusts the applet (and whether the decision is to be remembered). It also asks if all applets from that developer are to be trusted. If the user agrees, the applet continues to load.

This is a much-simplified description of signed applet security. The following Web sites contain further details:

```
http://www.suitable.com/Doc_CodeSigning.shtml
http://developer.netscape.com/docs/manuals/signedobj/trust/index.htm
```

11.2 Host On-Demand SSL support

Host On-Demand can ensure the privacy of communications through the use of the Secure Sockets Layer (SSL) protocol when connecting to SSL-capable Telnet servers. Host On-Demand implements SSL Version 3 to provide message privacy and integrity. This section describes how Host On-Demand has implemented SSL.

The key part of SSL negotiation is the client's ability to trust the certificate presented by the server, and the server's ability to trust the certificate presented by the client.

Trusted CA public certificates

For Host On-Demand clients, the public certificates of the trusted CAs are stored in one of three places:

- WellKnownTrustedCAs.class file
- CustomizedCAs.p12 file
- Microsoft cryptographic database

Client certificates

Host On-Demand has two places to look for the client certificate if required:

1. A password-protected PKCS12 file accessed through the local file system, or in a URL.

   This is the same level of support as was provided by Host On-Demand Version 4 and the initial release of Host On-Demand Version 5. The URL protocols you can use depend on the capabilities of your browser. Most browsers support HTTP, HTTPS, FTP, and FTPS.

2. A client certificate accessible through the Microsoft cryptographic API (CAPI).

   The Microsoft cryptographic API is the security interface used by Internet Explorer to access its certificates, client or server, and is available only on Windows platforms. Microsoft introduced this API with Internet Explorer Version 5.

11.2.1 Java class files

There are two key Java class files that are used by the Host On-Demand emulation clients when negotiating SSL sessions with Telnet servers: WellKnownTrustedCAs.class and CustomizedCAs.p12. The WellKnownTrustedCAs.class file contains the public certificates of all the CAs that Host On-Demand trusts. The CustomizedCAs.p12 file contains the certificates of unknown CAs and self-signed certificates.

The WellKnownTrustedCAs.class file is supplied by Host On-Demand and is not to be modified by the customer. If a self-signed certificate or a certificate from a unknown authority (CA) is to be used, the CustomizedCAs.p12 must be created or updated by the customer.

Both the WellKnownTrustedCAs.class file and the CustomizedCAs.p12 files are stored in the publish directory. All Host On-Demand download clients, including cached clients, obtain or refresh these files from the server when the applet is loaded.

Locally installed clients have the WellKnownTrustedCAs.class file installed on the workstation during product installation. A CustomizedCAs.p12 file is not installed by default, so if a locally installed client requires a certificate from a unknown CA or self-signed certificate, it must be created. The recommended method is to send the certificate to the client, and have the user create the CustomizedCAs.p12 file at the client. Refer to 12.2.4, “Making server certificates available to clients” on page 476. To create the CustomizedCAs.p12 file on the Host On-Demand server on OS/390, refer to “Creating the CustomizedCAs.p12 file on the server” on page 104.

Note: Prior to Version 8, Host On-Demand used the file CustomizedCAs.class to store self-signed certificates or certificates from an unknown authority (CA). Even though Host On-Demand Version 8 uses a CustomzedCAs.p12 file, the CustomizedCAs.class file may be needed for older clients. See 12.2.4, “Making server certificates available to clients” on page 476 for more information.

11.2.2 Microsoft cryptographic service provider database

Starting with Version 5.03, Host On-Demand provided an enhancement that allows the administrator to enable Host On-Demand to use the cryptographic API interface to store client certificates and public key certificates for CAs into the Microsoft cryptographic service provider database, hereafter referred to as the cryptographic database. This function has been tested and is supported on the following platforms:

- Windows 98
- Windows NT 4.0
- Windows 2000
- Windows Millennium Edition

The use of this interface provides simplification and usability improvements. All user prompting and card access for client authentication can be performed by the CAPI software. When selected, the Host On-Demand client receives a list of available client certificates and security providers, then presents the list to the user for selection to send to the server. As long as the Microsoft cryptographic database is installed, the option is available on both Netscape and Internet Explorer browsers, and is the preferred interface for Microsoft Internet Explorer.

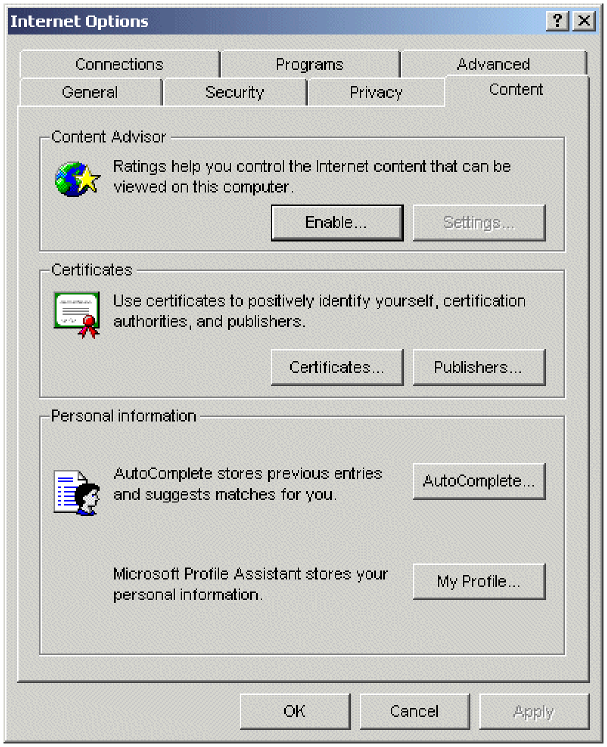
Through the use of the Microsoft cryptographic service provider database, not only do you have access to the client certificates, but to the CA certificates trusted by the browser as well. Therefore, if the Telnet server is using a certificate by a CA unknown to Host On-Demand, but known to the cryptographic database, then you can use the certificate located in the cryptographic database, thus eliminating the need to add the signer certificate to the CustomizedCAs.p12 file.

Many of the smart card readers are CAPI-compliant. By leaving hardware-level smart card processing to the CAPI and vendor interfaces, IBM is able to support new security devices without changing the Host On-Demand code. For instance, if a new thumbprint reader device becomes available, Host On-Demand will be able to access it through the use of the CAPI or the vendor interfaces without realizing it is not a smart card.

Viewing certificates

Certificates that are registered in the cryptographic database can be displayed in the following way:

1. Start the Internet Explorer 5.x browser.
2. Select **Tools -> Internet Options**.
3. Select the **Content** tab in the Internet Options window, as shown in Figure 11-1.



Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates to positively identify yourself, certification authorities, and publishers.

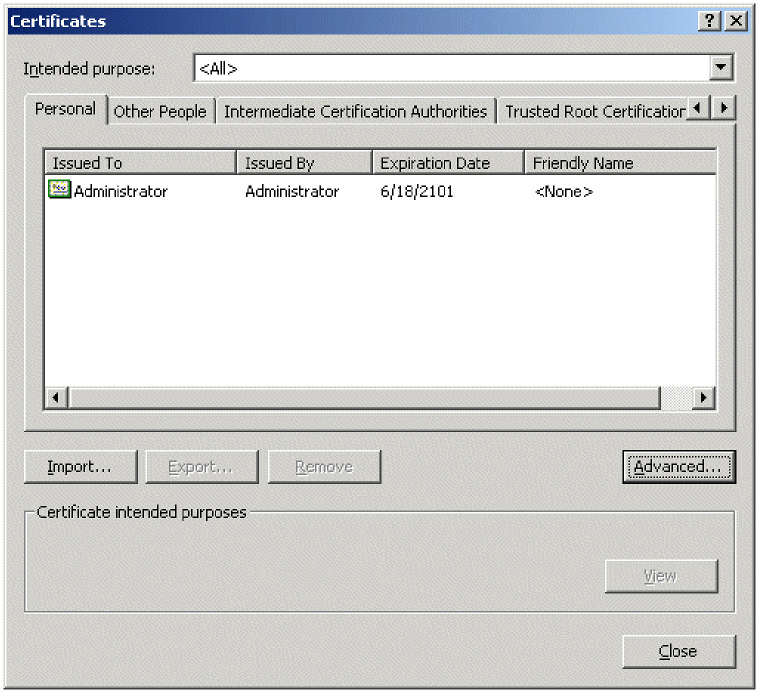
Personal information

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Figure 11-1 Internet Explorer Content tab

4. In the Content tab, click **Certificates**.
5. In the Certificates window shown in Figure 11-2, select the **Personal** tab. The certificates are displayed that will appear in the drop-down list on the Host On-Demand session configuration window and the Server Requesting Certificate window. If the certificate is not in this list, it will be obtained from either the WellKnownTrustedCAs.class file or the CustomizedCAs.p12 file.


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiration Date	Friendly Name
Administrator	Administrator	6/18/2101	<None>

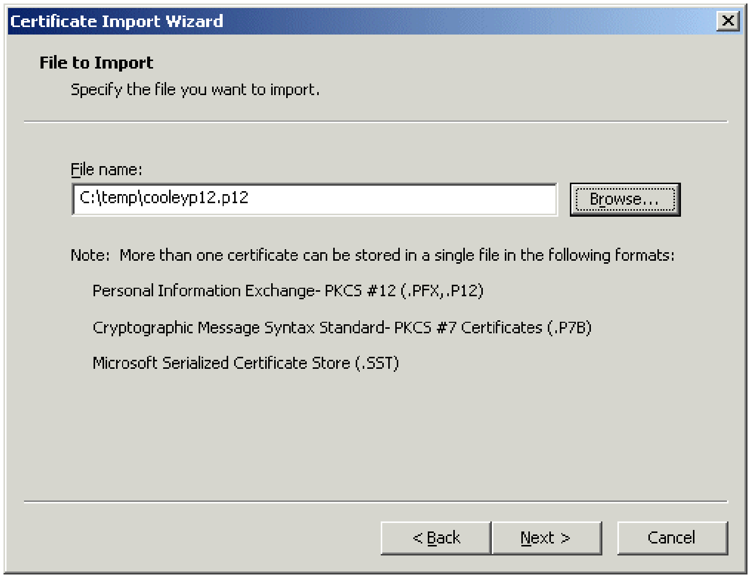
Figure 11-2 Personal certificate window

Adding a personal certificate

There are some security issues you need to be aware of when you add your personal certificate to the cryptographic database. The following instructions will assist you in the process. Please note that this procedure was developed using Microsoft Internet Explorer Version 5.5:

1. Start the Internet Explorer Version 5 browser.
2. Select **Tools -> Internet Options**.
3. Select the **Content** tab in the Internet Options window.
4. In the Content window, click **Certificates**.
5. Make sure you have selected the **Personal** tab, as shown in Figure 11-2, then click **Import** to start the process of adding your personal certificate to the database.
6. Click **Next** on the wizard startup window.

7. Enter the location of your personal certificate. You may click **Browse** to navigate to and select the file, or you may just type the location into the input field (see Figure 11-3). When completed, click **Next**.


Certificate Import Wizard
File to Import
Specify the file you want to import.
Browse...
< Back
Next >
Cancel

File name: C:\temp\cooleyp12.p12

Note: More than one certificate can be stored in a single file in the following formats:

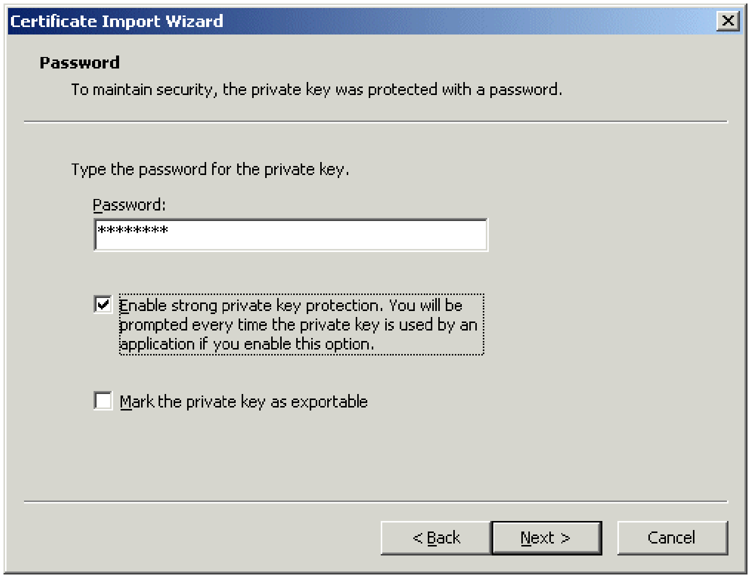
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Figure 11-3 Import certificate

8. You must enter your password for your personal certificate in the entry field as shown in Figure 11-4. If you select the first check box, then the browser will take an active role in prompting you for permission to use the certificate.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

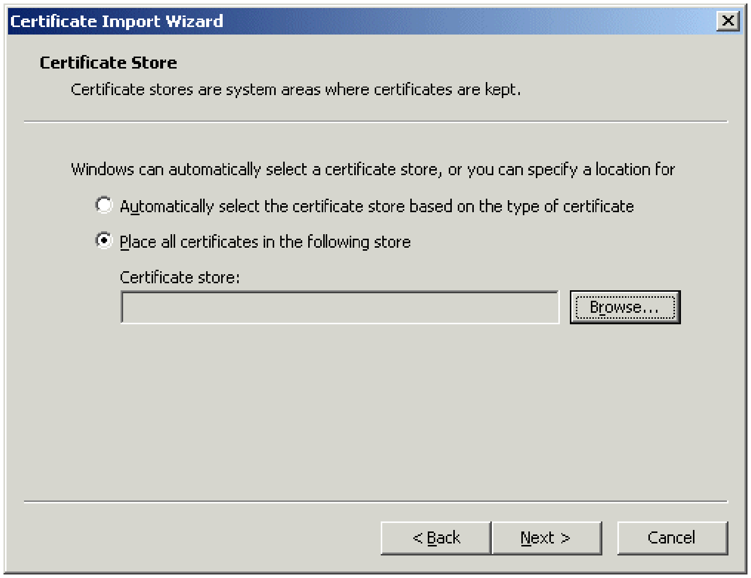
Password:
****

☑ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark the private key as exportable

Figure 11-4 Prompt for certificate password

9. Click **Next** to continue to the next window shown in Figure 11-5.You should specify that the certificate is to be stored in the Personal store by selecting the second radio button as shown in Figure 11-5, then click **Browse**, and select **Personal** from the resulting list as shown in Figure 11-6.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

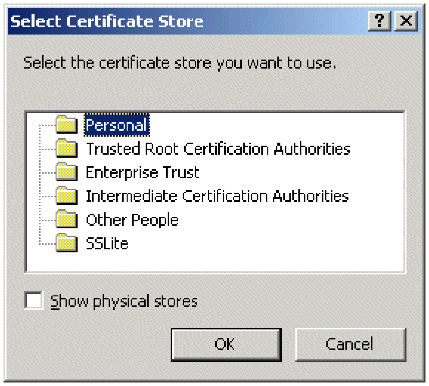
Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Figure 11-5 Certificate store



Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Other People
- SSLite

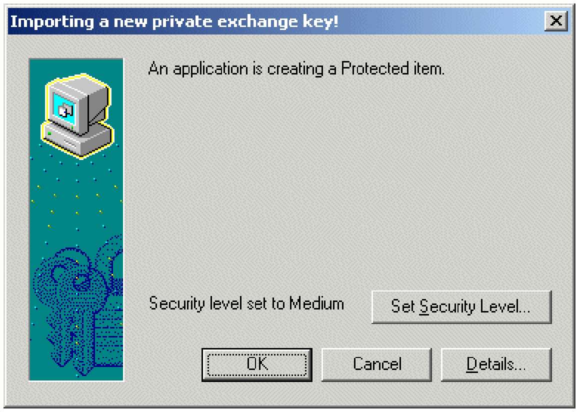
□ Show physical stores

Figure 11-6 Select Personal certificate store

10.Click **OK** and then **Next** to proceed to the last window of the wizard where you will click **Finish**.

11.If you selected the second check box in Figure 11-4 on page 416, then you are finished.

12. If you selected the first check box, then you will be presented with the window shown in Figure 11-7.



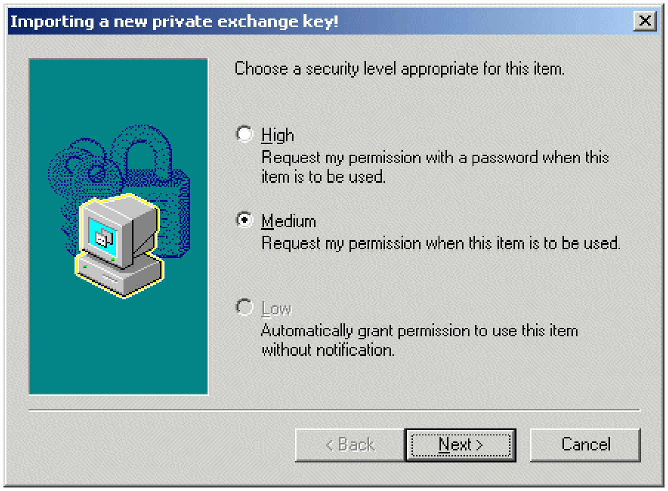
Importing a new private exchange key!

An application is creating a Protected item.

Security level set to Medium

Figure 11-7 Importing a private exchange key with security wizard

13. Click **Set Security Level** in the window shown in Figure 11-7 to set the desired security level for this certificate. You will be presented with three choices as shown in Figure 11-8.



Importing a new private exchange key!

Choose a security level appropriate for this item.

○ High
Request my permission with a password when this item is to be used.

● Medium
Request my permission when this item is to be used.

○ Low
Automatically grant permission to use this item without notification.

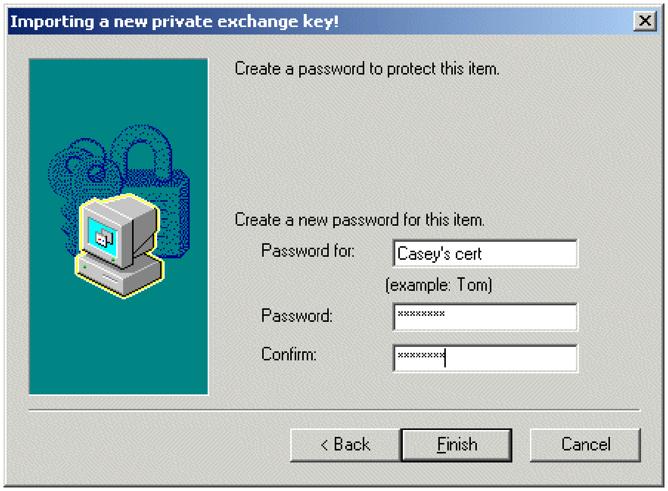
Figure 11-8 Choose security level

Here are the choices:

– If you select the default of **Medium**, you will be notified with a pop-up window that an application (Microsoft Internet Explorer) is requesting access to the protected file. When you click **OK**, this will allow Host

On-Demand to present the certificate to the Telnet server. Clicking **Cancel** will not allow Host On-Demand access to the certificate and Host On-Demand will present an error window. When you clear the error window, Host On-Demand will then prompt you for the certificate password.

- If you choose **High security** then you will be prompted (as shown in Figure 11-9) to provide a common name for your certificate and the password to be used when accessing it. Remember, this password is not the same as the certificate password. Click **Finish** and then **OK**.


Importing a new private exchange key!

Create a password to protect this item.

Create a new password for this item.

Password for: Casey's cert

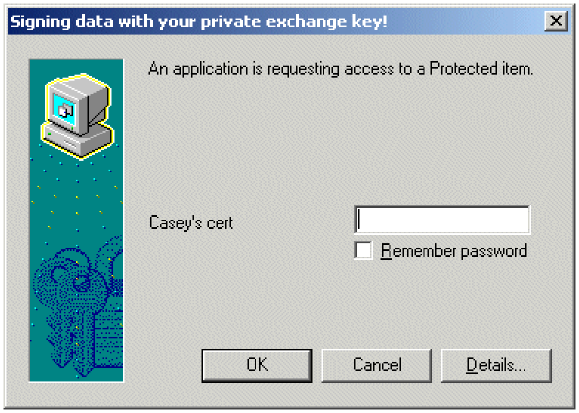
(example: Tom)

Password: ********

Confirm: ********

Figure 11-9 Create database password

- If **High security** is selected, the user will be prompted at runtime to provide a password (see Figure 11-10) in order to release the certificate. Notice that there is a check box to remember the password.



Signing data with your private exchange key!

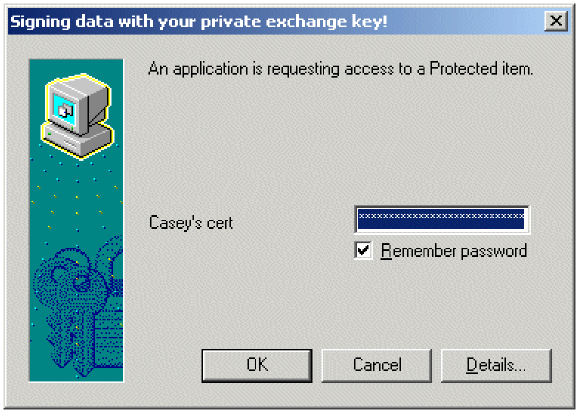
An application is requesting access to a Protected item.

Casey's cert

□ Remember password

Figure 11-10 Cryptographic password prompt

- If the check box is selected, then the system will remember the password and the next time the certificate is accessed, the prompt window shown in Figure 11-11 will appear, and all the user needs to do is click **OK**.



Signing data with your private exchange key!

An application is requesting access to a Protected item.

Casey's cert xxxxxxxxxxxxxxxxxxxxxxxxxx

☑ Remember password

Figure 11-11 Cryptographic remembered password

Recommendation

Implementation of the cryptographic database depends upon a user model that requires each user of the system to log in to the Windows system with a unique ID. If multiple users use the same Windows user ID, then they will share the same copy of the cryptographic database and thus each user will have access to all client certificates.

11.3 Host On-Demand SSL implementations

SSL is supported by all Host On-Demand emulator clients, 3270, 5250, and VT, whether they are locally installed, cached, or downloaded clients. There are three ways to use SSL with the emulator clients:

- Basic SSL
- Server authentication
- Client authentication

11.3.1 Basic SSL

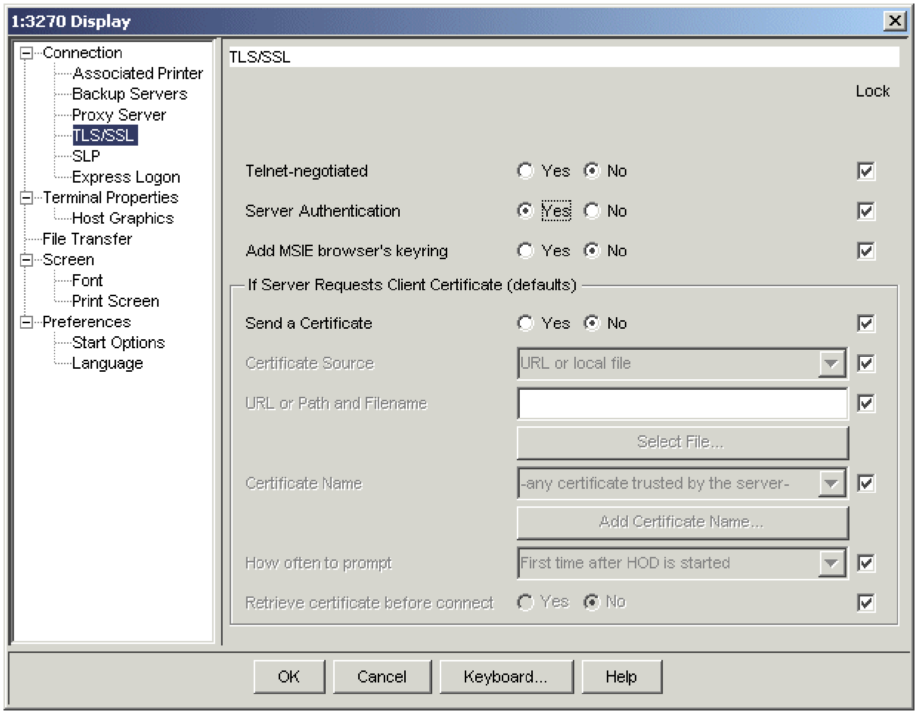
By default, when SSL is enabled for the Host On-Demand client, a basic SSL session is established. The server will present its certificate to the client during the negotiation process; refer to “Establishing secure communications with SSL” on page 1040. With basic SSL enablement, all that is required is that the client recognizes that the certificate is signed by an authority that it trusts.

If the client is running on a Windows platform and the session properties have the MSIE browser keyring file enabled, then the Microsoft cryptographic database is checked first to determine if the signer is trusted. If the signer certificate is not found in the cryptographic database, the cryptographic database is not enabled, or the client is not running on a Windows platform, then the WellKnownTrustedCAs.class file followed by the CustomizedCAs.p12 files will be checked. If the signer is not found in any of these repositories, the session is rejected. If the signer is found, the session is established.

11.3.2 Server authentication

Encrypting the data exchange between the client and the server does not guarantee the client is communicating with the correct server. To help avoid this danger, you can enable server authentication. Server authentication is a process where the client validates that it is communicating with the correct server before the session may be established. When implementing server authentication, the client must trust the server’s certificate before the session will be initiated.

Server authentication is not enabled by default, and must be selected on the TLS/SSL selection as shown in Figure 11-12.



TLS/SSL

		Lock
Telnet-negotiated	○ Yes ● No	☑
Server Authentication	● Yes ○ No	☑
Add MSIE browser's keyring	○ Yes ● No	☑

If Server Requests Client Certificate (defaults)

Send a Certificate	○ Yes ● No	☑
Certificate Source	URL or local file	☑
URL or Path and Filename		☑
	Select File...	
Certificate Name	-any certificate trusted by the server-	☑
	Add Certificate Name...	
How often to prompt	First time after HOD is started	☑
Retrieve certificate before connect	○ Yes ● No	☑

Figure 11-12 Enabling server authentication

When **server authentication** is selected, a secure session is negotiated as described in “Establishing secure communications with SSL” on page 1040. However, the Host On-Demand client immediately looks at the Common Name field of the server’s certificate to determine if the host name of the server presenting the certificate is stored in the Common Name field of the certificate.

Using one or more Java Virtual Machine (JVM) calls, the client obtains all IP numeric addresses associated with the Common Name in the server’s certificate. Next, JVM calls are made requesting all IP numeric addresses associated with the server as specified in the destination field of the session properties definition. When the results of both searches are complete, the client compares the two lists of addresses looking for at least one IP address that appears in both lists. If any IP address appears in both lists, the connection continues and data can be sent; however, if no IP address appears in both lists, then the connection is terminated, and an error generated to the session status line. For server authentication to work, a DNS must be available that can resolve these addresses, or the server address must be defined in the TCP/IP hosts file.

For server authentication to be valid and to give a positive result, two conditions must be met if you are not using the cryptographic database:

1. The client must be locally installed.

   A client downloaded using HTTP cannot be trusted for server authentication because the WellKnownTrustedCAs.class file and the CustomizedCAs.p12 file are downloaded from the server.

2. The Common Name in the server's certificate must match its Internet name.

The crucial step in the process is when the client checks its list of trusted CAs and self-signed certificates. For a locally installed client, the list is kept on the local hard disk. This is considered adequately secure. However, for a download client, on which the client is a browser that downloads all its code from the server using HTTP(S), the only place the browser can look for the list of trusted CAs or self-signed certificates is on the server from which it has just downloaded the certificate. If that server is an intruder, or if an intruder can intercept and alter data passed from the server to the client, security is breached.

11.3.3 Client authentication

The server may also want to restrict access only to clients that the server trusts. The process of client authentication has the Telnet server requesting a certificate from the client to verify that the client is who it claims to be, and that it is allowed access to the server. Not all servers support client authentication, including the Host On-Demand Redirector. To configure client authentication, you must obtain certificates for clients, send the certificates to the clients, and configure the clients to use client authentication.

Client authentication is similar to server authentication except that with client authentication the Telnet server requests a certificate from the client to verify that the client is who it claims to be. The certificate must be an X.509 certificate and signed by a Certificate Authority (CA) trusted by the server. You can only use client authentication when a server requests a certificate from a client. Not all servers support client authentication, including the Host On-Demand Redirector.

In order to use client authentication you must:

- Obtain a client certificate.
- Transfer the certificate available to the client by either sending it directly, or making it available through a shared LAN drive or a secure HTTPS connection.
- Always send the password for the certificate through a separate out-of-band secure method so as not to compromise the certificate.

The certificate can be kept in the client's browser, a dedicated security device such as a smart card; or in a local or network-accessed file in PKCS12 or PFX format, which is protected by a password.

When a certificate expires, follow the renewal procedures specified by the CA for that certificate.

11.3.4 TN3270 client

The 3270 display and printer clients support SSL. The Host On-Demand 3270 display session supports all three types of SSL sessions:

- Basic
- Server authentication
- Client authentication

The 3270 printer session supports the following two types of file transfer:

- Host File Transfer (IND$FILE)

  The IND$FILE mode uses the 3270 data stream to transfer the data; therefore, if the emulator session is encrypted so is the file transfer data.

- FTP

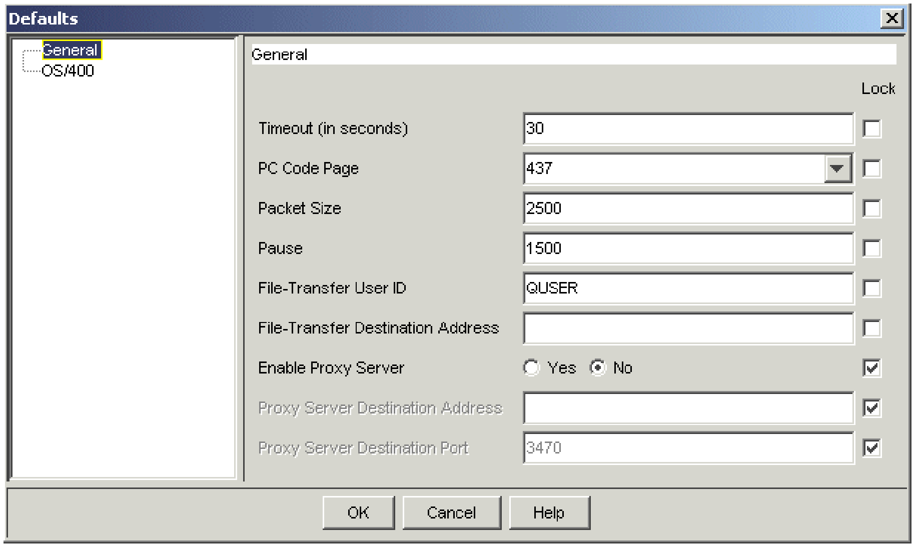
  The FTP option is the same method as deployed with the FTP client described in 11.3.7, "FTP client" on page 426.

11.3.5 TN5250 client

The TN5250 emulator client supports SSL sessions. The Host On-Demand 5250 emulator client supports all three types of SSL sessions: basic, server authentication, and client authentication. The 5250 emulator supports two types of file transfer:

- Host file transfer
- FTP

Host file transfer with TN5250 does not use the 5250 data stream to do the file transfer as does the TN3270 host file transfer (IND$FILE). It uses a file transfer method derived from the Host Servers Licensed Product (57xxSS1/Option 12). When configuring host file transfer, the window shown in Figure 11-13 is displayed.



		Lock
Timeout (in seconds)	30	□
PC Code Page	437	□
Packet Size	2500	□
Pause	1500	□
File-Transfer User ID	QUSER	□
File-Transfer Destination Address		□
Enable Proxy Server	○ Yes ● No	☑
Proxy Server Destination Address		☑
Proxy Server Destination Port	3470	☑

Figure 11-13 Configure 5250 host file transfer

If you select **No** for Enable Proxy Server, then the file transfer operation will occur to the destination file transfer address using the same security as the 5250 client. This means if the 5250 session is not encrypted, then file transfer data will not be encrypted, but if the 5250 session is encrypted, the file transfer data will also be encrypted using server authentication.

If you select **Yes** for Enable Proxy Server, then the file transfer operation from the client to the O/S400 Proxy Server will not be encrypted. Refer to Chapter 10, “OS/400 Proxy” on page 397 for details on the operation and configuration of the O/S400 Proxy Server.

The FTP option is the same method as deployed with the FTP client described in 11.3.7, “FTP client” on page 426.

11.3.6 VT client

The VT client supports SSL and SSH. Unless the system you will be connecting to supports SSL on the VT session, you must use a redirector that does, such as the Host On-Demand Redirector or the Communications Server for AIX Telnet Redirector. To be able to use SSH, the system you are trying to connect to must support SSH, a redirector may not be used.

11.3.7 FTP client

The FTP client supports SSL and Secure Shell FTP for secure file transfers (sftp). To be able to use SSH, the system you are trying to connect to must support SSH. A redirector may not be used.

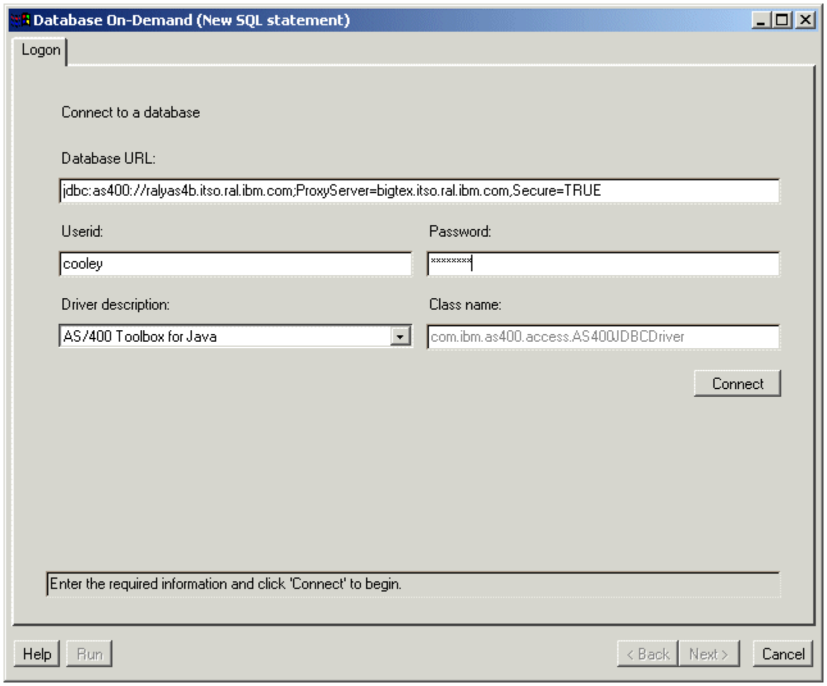
11.3.8 Database On-Demand client

The Database On-Demand client supports the use of SSL. Figure 11-14 illustrates the ;Secure=TRUE parameter that may be added to the Database URL when initiating a database query. If you wish to use the O/S400 Proxy Server you need to add:

```
;Proxy Server=ralyas4c.itso.ral.ibm.com
```

to the Database URL, where ralyas4c.itso.ral.ibm.com is the O/S400 Proxy Server destination address.

Note: If you are using the OS/400 proxy for port reduction, the session between the client and the proxy will not be encrypted even if the secure parameter is specified.



Database On-Demand (New SQL statement)

Logon

Connect to a database

Database URL: jdbc:as400://ralyas4b.itso.ral.ibm.com;ProxyServer=bigtex.itso.ral.ibm.com,Secure=TRUE

Userid: cooley

Password: ********

Driver description: AS/400 Toolbox for Java

Class name: com.ibm.as400.access.AS400JDBCDriver

Enter the required information and click 'Connect' to begin.

Figure 11-14 Database On-Demand configuration

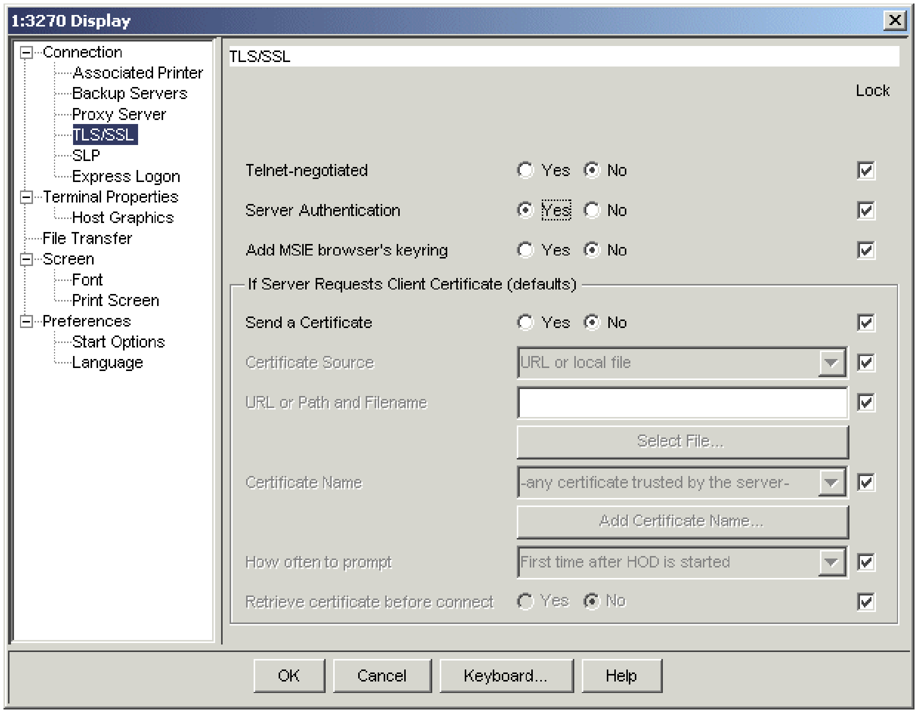
Note: If you are using the Netscape browser and you see this message when logging on:

```
Please disable the JIT compiler and restart the browser.
```

you must stop your browser, rename the Netscape jit*.dll file and restart your browser. This file is located in the `\program files\netscape\communicator\program\java\bin\` directory.

11.4 Defining a secure Telnet session

There are many options available when enabling security for a Telnet session. In order to understand the interrelationships and operational implications, each of the settings for each option as shown in Figure 11-15 is examined.



TLS/SSL

Lock

Telnet-negotiated ○ Yes ● No ☑

Server Authentication ● Yes ○ No ☑

Add MSIE browser's keyring ○ Yes ● No ☑

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No ☑

Certificate Source: URL or local file ☑

URL or Path and Filename: ☑

Certificate Name: -any certificate trusted by the server- ☑

How often to prompt: First time after HOD is started ☑

Retrieve certificate before connect ○ Yes ● No ☑

Figure 11-15 Session configuration for security

Additional information on session configuration for security can be found at “3270/5250 TLS/SSL selection” on page 291 and “Session configuration” on page 1045.

11.4.1 Enable security

The first and most important option is whether or not to enable security. If you select **Telnet** as the protocol to be used at the Connection selection, the options in this TLS/SSL configuration window will be unavailable. Thus, the client will not attempt to do any SSL, and all transmissions will be in the clear. If you selected either **Telnet - TLS** or **Telnet - SSL only**, the options on this window become available, and at a minimum basic SSL (see 11.3.1, “Basic SSL” on page 421) will be attempted.

11.4.2 Security protocol

In addition to SSL, Host On-Demand supports version 1.0 of the Transport Layer Security (TLS) protocol. This drop-down menu allows you to select which security protocol to use for this session:

- Telnet - TLS

  Enables Transport Layer Security (TLS). TLS version 1.0 is the default security protocol for Host On-Demand clients. Note that TLS allows security negotiations from TLS version 1.0 to SSL version 3.0.

- Telnet - SSL only

  Enables SSL version 3.0 security. Select this protocol only if the server cannot correctly negotiate a TLS connection.

11.4.3 Telnet-negotiated session

This option is not available unless you first enable security. Selecting a Telnet-negotiated session determines if the security negotiations between the client and the Telnet server are done on the established Telnet connection, or on a TLS connection prior to the Telnet negotiation. For the client to use this feature, the Telnet server must support TLS-based Telnet Security. The other options are valid regardless of whether Telnet-negotiated is set to `Yes` or `No`.

The other SSL options are valid regardless of whether the Telnet-negotiated radio button is Yes or No.

If you click **Yes**, then the Telnet protocol defined in IETF RFC TLS-based Telnet Security will be used to negotiate the SSL security after the Telnet connection is established. This support is only applicable with a Telnet server that supports TLS-based Telnet Security.

If you click **No**, the traditional SSL negotiations will be done on an SSL connection with the server, and subsequently the Telnet negotiations with the server will be done.

11.4.4 Server authentication

The default here is **No**, but should you click **Yes**, then the client will perform the server authentication process as documented in 11.3.2, “Server authentication” on page 421.

11.4.5 Add MSIE browser’s keyring

Clicking **Yes** for this parameter allows the client, when running on a Windows platform, to search the cryptographic database when validating the server’s certificate. If the CAs public certificate is not found in the cryptographic provider database, then the applet will look in the WellKnownTrustedCAs.class file followed by the CustomizedCAs.p12 file if necessary to validate the certificate.

This setting is valid only on a Windows platform. The cryptographic database is available to the Host On-Demand client regardless of the browser being used by the client. This setting has no effect on the client authentication process.

11.4.6 Client authentication

There are many options available if client authentication is to be deployed. First and foremost the session must be configured to respond to the Telnet server with a client certificate. This is done by clicking **Yes** to the Send a Certificate option as shown in Figure 11-15. Once you click **Yes**, then the remaining options in this section of the window are enabled.

Certificate source

There are two places that the Host On-Demand client will look for the X.509 certificate:

- The client's local file system, which includes any configured LAN, NFS, AFS®, etc. drives, or from a standard URL
- A security device, such as a smart card, or from the cryptographic database

If you select **Certificate in URL or local file system**, then you may enter the location where the certificate is found into the URL, or Path and Filename fields. You may use **Select File** to browse your file system to find the file.

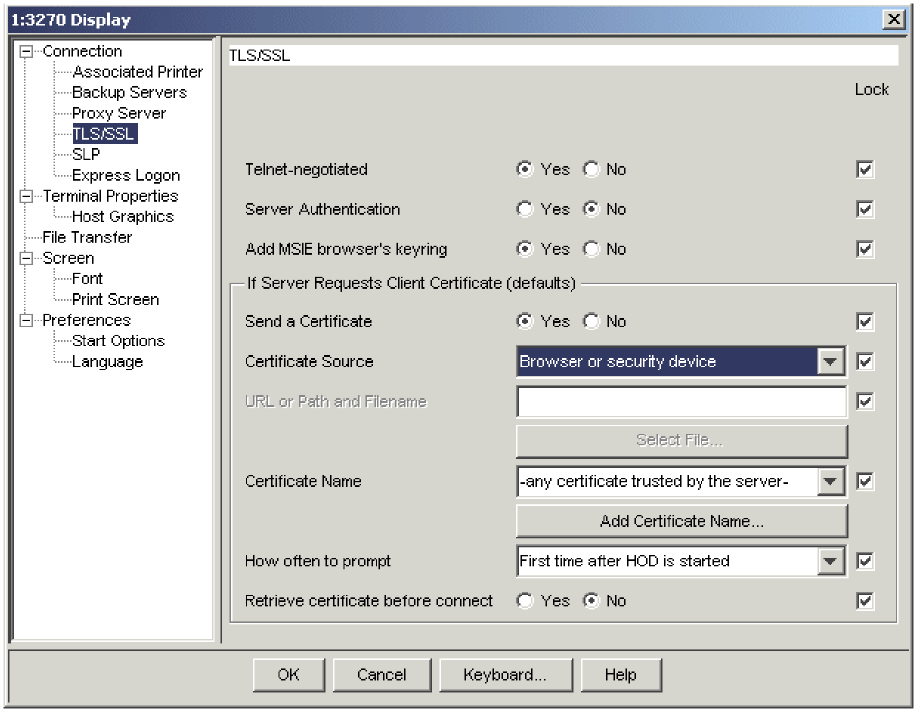
Certificate name

This option will become active when you indicate the certificate is in the browser or security device. Host On-Demand will read the cryptographic database from the machine on which this function is being performed. If you select the default entry, **-any certificate trusted by the server-**, Host On-Demand will search the list returned at runtime, and select the first certificate recognized by the server. The operator also has the option to view the certificates found in the cryptographic database at configuration time, and selects one of them as well. This option is fine if the operator is operating on the settings for his own session, but if the operator is an administrator, there is no way to know beforehand what certificates will be available on any given client that will use this setting. For administrator operations, refer to "Selecting the client certificate" on page 431.

When a server requests a certificate, the client will check the status of the Send Certificate option set in the session properties file. If it is set to `No`, a certificate will not be sent and the session may be denied. If the option is set to `Yes`, then the certificate will be located as per the settings in the session configuration file (see Figure 11-15 on page 428) and the certificate is sent to the server. The user may be prompted for the password of the certificate before it is sent. Finally, the server makes a connection if the client's certificate can be trusted.

Selecting the client certificate

When defining the sessions and selecting that the certificate will be found in the browser or security device (see Figure 11-16), the administrator has the ability to set a mask that will be used to identify the proper certificate from the cryptographic database.



1:3270 Display

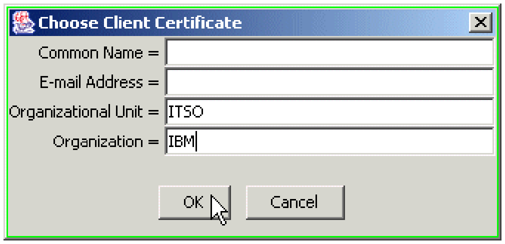
- Connection
  - Associated Printer
  - Backup Servers
  - Proxy Server
  - TLS/SSL
  - SLP
  - Express Logon
- Terminal Properties
  - Host Graphics
- File Transfer
- Screen
  - Font
  - Print Screen
- Preferences
  - Start Options
  - Language

TLS/SSL

		Lock
Telnet-negotiated	● Yes ○ No	☑
Server Authentication	○ Yes ● No	☑
Add MSIE browser's keyring	● Yes ○ No	☑
If Server Requests Client Certificate (defaults)		
Send a Certificate	● Yes ○ No	☑
Certificate Source	Browser or security device	☑
URL or Path and Filename		☑
	Select File...	
Certificate Name	-any certificate trusted by the server-	☑
	Add Certificate Name...	
How often to prompt	First time after HOD is started	☑
Retrieve certificate before connect	○ Yes ● No	☑

Figure 11-16 Using certificate from browser

The administrator sets the mask by clicking **Add Certificate Name.** This results in a window (Figure 11-17) that allows the administrator to specify a mask that will be used in selecting which certificate from the client's cryptographic database will be selected.



Choose Client Certificate

Common Name =

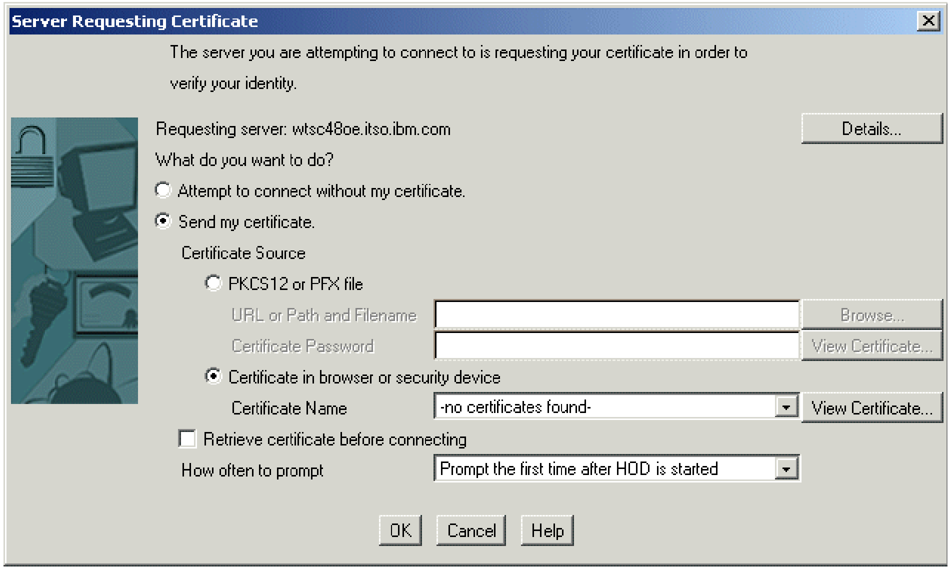
E-mail Address =

Organizational Unit = ITSO

Organization = IBM

Figure 11-17 Set up client certificate mask

The mask is not case sensitive and wild cards are not allowed. When the certificate is requested, the cryptographic database is searched, and the first valid certificate to fit all the components specified is sent. If no certificates are found, the client displays the window shown in Figure 11-18, prompting the end user for further action.



Server Requesting Certificate

The server you are attempting to connect to is requesting your certificate in order to verify your identity.

Requesting server: wtsc48oe.itso.ibm.com

What do you want to do?

○ Attempt to connect without my certificate.

● Send my certificate.

Certificate Source

○ PKCS12 or PFX file

URL or Path and Filename

Certificate Password

● Certificate in browser or security device

Certificate Name: -no certificates found-

□ Retrieve certificate before connecting

How often to prompt: Prompt the first time after HOD is started

Figure 11-18 No certificates found

The option to specify a mask is available only to the administrator, because if you are the user, you should see the list of all of your certificates, but if you are the administrator, there is no way you can see all the certificates on the client's computer.

Note: Using the mask is one technique that may be used to restrict access to valid certificate holders based upon an organizational requirement.

How often to prompt

This drop-down box allows you to control the timing of Host On-Demand prompts for client certificates. The four options are:

- Prompt only once, storing preferences on client. If your client stores preferences locally (specified when the client HTML file was created through the Deployment Wizard), the client is prompted for the password the next time the connection is made, but never after that, unless the connection attempt fails. This option is only available on the client's configuration window.

- Prompt on each connection. Client is prompted each time a connection is made to the server.
- Prompt the first time after Host On-Demand is started. Client is prompted only once each time the Host On-Demand server is started.
- Prompt the first time after Host On-Demand is started. Client is prompted only once each time the Host On-Demand server is started.

If you specified URL or local file for the certificate source, then the do-not-prompt option will be available to the client. If the certificate is stored in the cryptographic database (browser), the no Host On-Demand password prompt is required, and you may select the **no-prompt** option. Host On-Demand will not prompt you for your certificate password; however, depending upon the options you selected when you stored your certificate, the cryptographic database may prompt or notify you. Refer to "Adding a personal certificate" on page 414 for more details.

Retrieve certificate before connecting

If you click **Yes** to retrieve a certificate before connecting (Figure 11-16 on page 431), the client will access its certificate before connecting the server, whether the server requests a certificate or not. If you click **No**, the client will access the certificate only after the server has requested it; depending on other settings, this may force the client to abnormally terminate the connection to the server, prompt the user, and then re-connect. It is recommended that you choose **Yes** if you will be authenticating with a Communications Server for OS/390 system; otherwise, unnecessary error messages may be generated.

11.5 Host On-Demand SSH support

Host On-Demand V8 added SSH support for VT display sessions and sftp.

11.5.1 SSH overview

The Secure Shell (SSH) is a set of protocols for implementing secure sessions over a non-secure network (such as a standard TCP/IP network). TLS/SSL and SSH are similar to each other, but different in the following ways:

- TLS was designed for HTTP (use of certificate).
- SSH was designed as a replacement of Telnet (more focus on user authentication).

Figure 11-19 illustrates the differences.

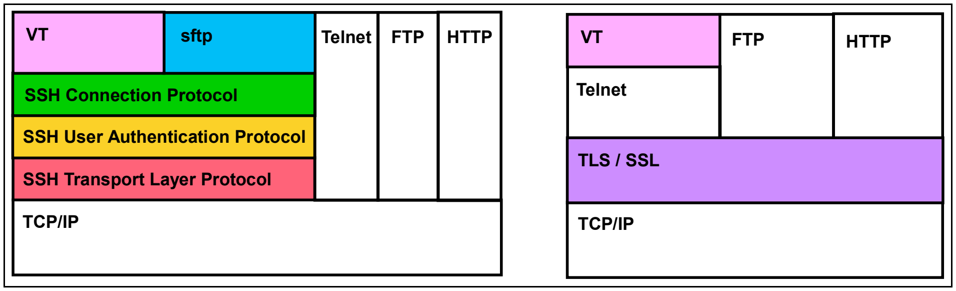


Figure 11-19 Differences between TLS and SSH

In order to use SSH, you must set up SSH server software on the host. Security features include the following:

- Secure remote login
- Strong authentication of server and client
- Several user authentication methods
- Encrypted terminal sessions
- Secure file transfers

SSH uses the well-known port 22.

11.5.2 SSH-Level and features supported by Host On-Demand

Host On-Demand supports SSH as an option on the following session types:

- VT Display sessions
- File Transfer (sftp) sessions. This is not *secure FTP* which uses TLS/SSL.

The implementation of SSH in Host On-Demand is a subset of SSH Version 2. Host On-Demand does not support earlier versions of SSH, such as Version 1.3 or Version 1.5.

The following subsections describe for each protocol in SSH Version 2.0 the features that Host On-Demand supports, or the features that Host On-Demand does not support:

- SSH Transport Protocol

  For the SSH Transport Protocol, Host On-Demand supports the algorithms shown in Figure 11-1 for both sending files (client to server) and receiving files (server to client).

Table 11-1 SSH Transport protocol - supported algorithms

Category	Algorithm supported
Compression	None
Encryption	3des-cbc
Data Integrity	hmac-sha1
Key Exchange	diffie-hellman-group1-sha1
Public Key	ssh-dss (same as DSA)

- SSH Authentication Protocol

  For the SSH Authentication protocol, Host On-Demand supports the following authentication methods:

  – Public key
  – Password

- SSH Connection Protocol

  Host On-Demand does *not* support the following features in the SSH Connection protocol:

  – X11 forwarding
  – Environment Variable Passing
  – Remote Command Execution
  – Windows Dimension Change Message
  – Signals
  – TCP/IP Port Forwarding

- SSH File Transfer Protocol (sftp)

  For the SSH File Transfer, Host On-Demand supports only binary file transfers; character-mode file transfers are not supported.

  Host On-Demand does not support the following features in the SSH File Transfer protocol:

  – Encoding of filenames in UTF-8 format
  – Newline extension
  – Operations that use symbolic links

For further information about basic TCP/IP security, refer to “Introduction to TCP/IP security” on page 1009.

11.5.3 Host On-Demand client requirements for SSH support

For SSH support, Host On-Demand requires the following configuration on the client workstation:

- A Java 2-enabled browser

  SSH is not supported with a Java 1 browser, because Java 1 does not support the Java Cryptography Extension.

- The Java Cryptography Extension (JCE)

  The JCE is included as part of the IBM 32-bit Runtime Environment (JRE) for Java 2, V1.4 (for Microsoft Windows platforms). This version of the Java 2 JRE is included with Host On-Demand, and can be downloaded by Windows platform clients from the Host On-Demand server. For more information, refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301.

  The JCE is also included in Sun Java 1.4.

  For Java 1.3 (IBM or Sun), the JCE is available as add-on from Sun.

  You cannot use Java 1.2.

11.5.4 Starting a session

Figure 11-20 shows the basic dataflow when a SSH session is started.

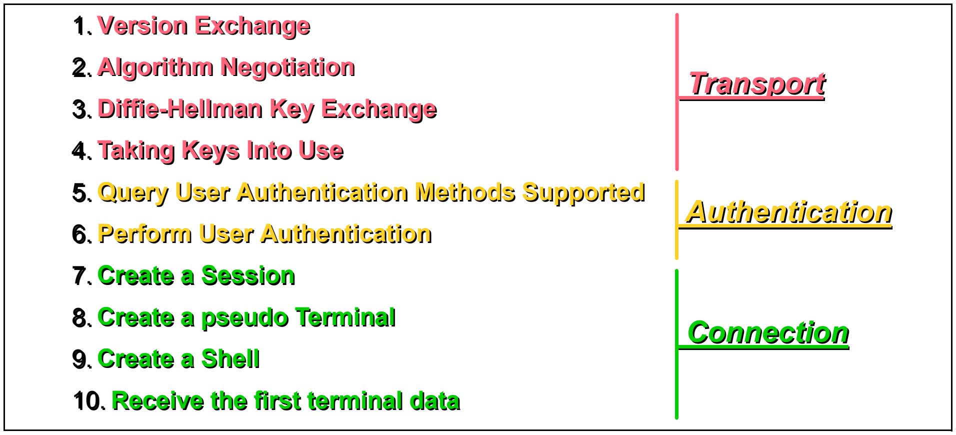

1. Version Exchange
2. Algorithm Negotiation
3. Diffie-Hellman Key Exchange
4. Taking Keys Into Use
5. Query User Authentication Methods Supported
6. Perform User Authentication
7. Create a Session
8. Create a pseudo Terminal
9. Create a Shell
10. Receive the first terminal data
Transport
Authentication
Connection

Figure 11-20 Session start

Please refer also to 11.5.7, “SSH trace example” on page 443.

11.5.5 Authentication for SSH

Host On-Demand allows both public-key authentication and password authentication to be configured on the client at the same time.

At runtime:

- If public-key authentication is configured, then Host On-Demand tries this type of authentication with the host first. If public-key authentication is not configured, or if it is configured and fails, then Host On-Demand moves on to password authentication.
- For password authentication, Host On-Demand looks for a password in the session configuration. If no password is found, Host On-Demand prompts the user for a password. Once a password is received, Host On-Demand then tries password authentication with the host.
- If password authentication fails, then Host On-Demand displays an error message.

Public-key authentication

Public-key authentication for SSH requires that the server knows the public key of the client. Here is an overview of the method for generating this public key and making it available to the server with Host On-Demand.

The basic flow of a public-key authentication is shown in Figure 11-21. The numbered items in the figure correspond to the following numbered steps.

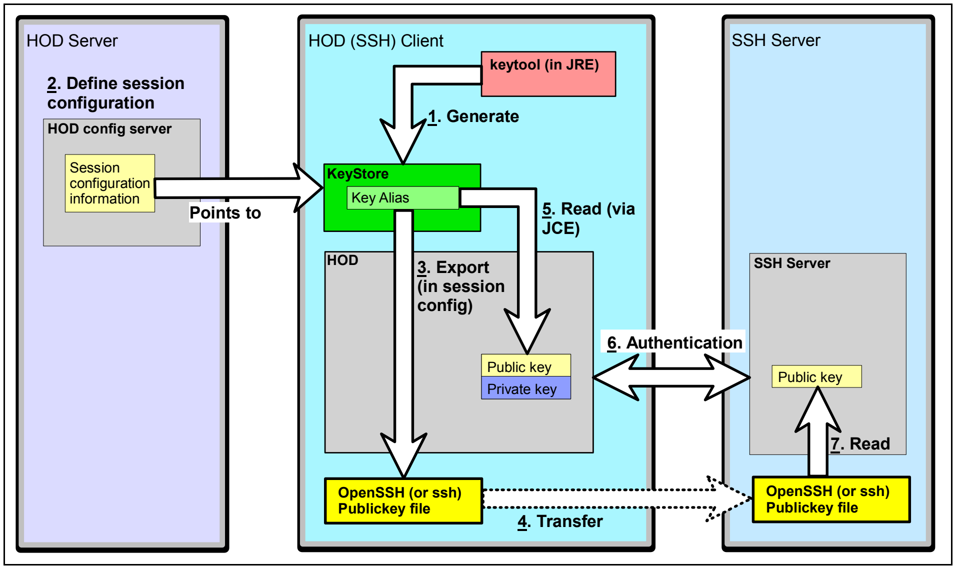


Figure 11-21 Public-key authentication

Here are the steps:

1. Use the HOD client's keytool utility in the JCE to generate a keystore containing a pair of keys for the client (a public key and a private key). To generate the keystore, invoke the keytool utility as follows:

   ```
   keytool -genkey
   ```

   For example, on a Windows platform you might type the following:

   ```
   c:\program files\ibm\java14\jre\bin\keytool.exe -genkey
   ```

   The keytool utility then prompts you for the following information:

   – A password for the keystore

   – Information routinely requested for public-private key pairs, including:

     - User's first and last name
     - Organizational unit
     - Organization
     - City or locality
     - State or province
     - Two-letter country code

   – A password for the public-private key pair, which might be the same as the password for the keystore

When invoked with only the **`-genkey`** option, as above, the keytool utility generates the items listed below. These are the default values generated by the keytool utility, and are also the default values expected by Host On-Demand configuration.

- A keystore with the name `.keystore`.
- By default, the keytool utility generates this file in the directory named in the Java system property user.home. For example, for the Microsoft Windows platform, the file would be generated in the following directory:
- `c:\Documents and Settings\username`
- Where `username` is the user name.
- In the keystore, a 1024-bit DSA key pair (a public key and associated private key) with the key alias mykey. Host On-Demand supports 1024-bit DSA keys only.

To generate a keystore with a non-default filename, key alias, store password, and alias password, invoke the keytool utility with the following command. (**Note** that the command appears in this document on two lines; however, you should type it all on one line.)

```
keytool -genkey -keystore MyKeystoreFile -alias MyAlias

        -storepass MyKeystorePassword -keypass MyKeyPassword
```

Example 11-1 shows the screen output if the keytool utility is used with personalized values.

Example 11-1 Screen output of the keytool utility

```
C:\Program Files\IBM\Java14\jre\bin>keytool -genkey -keystore
c:\temp\keystorefile -alias atalias -storepass atpasswd -keypass atpasswd
What is your first and last name?
  [Unknown]:  Achim Tepper
What is the name of your organizational unit?
  [Unknown]:  ITSO
What is the name of your organization?
  [Unknown]:  IBM
What is the name of your City or Locality?
  [Unknown]:  Raleigh
What is the name of your State or Province?
  [Unknown]:  NC
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Achim Tepper, OU=ITSO, O=IBM, L=Raleigh, ST=NC, C=US correct?
  [no]:  yes

C:\Program Files\IBM\Java14\jre\bin>
```

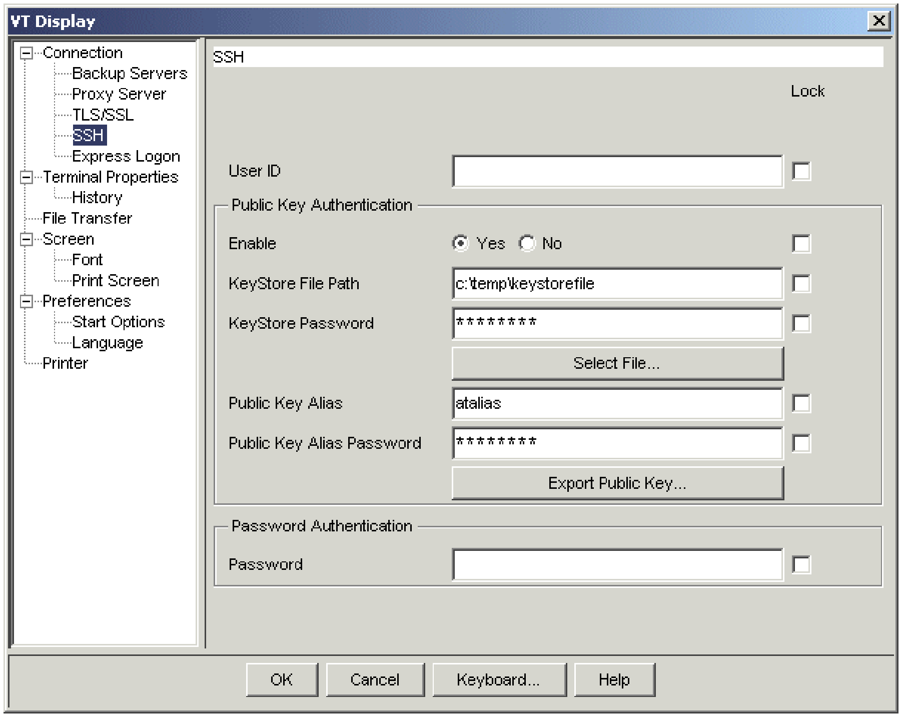
Run the keytool utility with no options specified to see all the possible options.

If you did not specify the proper directory and filename for the keystore file when running the keytool utility already, place the keystore file in the proper subdirectory on the client workstation. As mentioned above, the default file name is .keystore, and the default subdirectory is the path stored in the user.home Java system property. In any case, you should use the same file name and path that you plan to specify in the session configuration. This may be a local drive, or any other drive reachable by the client such as a network drive.

2. At the Host On-Demand server, configure the Host On-Demand session parameters for SSH. As mentioned above, two Host On-Demand session types support SSH:

   – VT Display
   – File Transfer (sftp)

   For a description on how to configure these sessions, please see “VT Display session” on page 309 and “FTP/sftp session” on page 322.



SSH

User ID □

Public Key Authentication

Enable ● Yes ○ No □

KeyStore File Path c:\temp\keystorefile □

KeyStore Password ******** □

Public Key Alias atalias □

Public Key Alias Password ******** □

Password Authentication

Password □

Figure 11-22 Completed SSH selection

You will need to specify the following information (or you can accept the default values):

- Path and file name for the keystore

  The default is the file .keystore in the directory pointed to by the Java system property user.home.

- Password for the keystore

  If no password is specified in the configuration then when the session is started, the Host On-Demand client will display a popup window prompting for the password.

- Key alias

  The default is `mykey`.

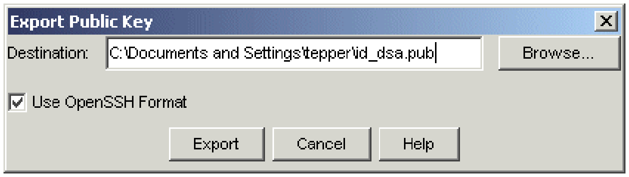
- Password for the key alias

  - If no password is specified, then when the session is started Host On-Demand will attempt to read the public key information using a null password (no password).
  - If the attempt to read the public key information using a null password fails, then the Host On-Demand client will attempt to read the public key information using the same password as the password for the keystore.
  - If the attempt to read the public key information using the KeyStore Password fails, then Host On-Demand client will prompt the user for the password.

3. For this step, one of the following is required:

   - The administrator has to log on at the client system.
   - The client user has to be able to access the session configuration. which means the fields at the SSH selection that deal with public-key authentication may not be locked by the administrator.

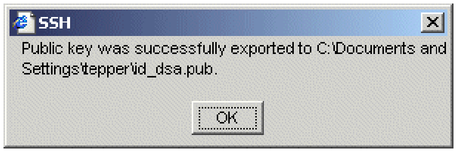
   Use the export Public Key utility in order to export the public key to a plain-text file. This utility is not a stand-alone utility but rather is integrated with the session configuration. To run the utility, go to the SSH configuration panel in the session configuration, the same panel where you specified the path and file name for the keystore, and click **Export Public Key**. Follow the instructions to export the public key to a plain text file.



Destination: C:\Documents and Settings\tepper\id_dsa.pub

☑ Use OpenSSH Format

Figure 11-23 Extracting the public-key



SSH

Public key was successfully exported to C:\Documents and Settings\tepper\id_dsa.pub.

Figure 11-24 Extracting the public-key - Completed

4. Transfer the plain text file to the system to which your VT or sftp session will later connect to. This is also the system where the SSH server is running. You should use a secure method for transferring the plain text file to that system, such as one of the following:

   – SSH file transfer (sftp)
   – Diskette

   The server configuration for public-key authentication differs depending on the vendor or source of the SSH support. Refer to the documentation for your SSH server software for information on how to configure the SSH server for the public-key authentication method.

   > **Attention:** Steps 3 and 4 need to be done on and for any client that will later use SSH secured sessions. This will cause a huge amount of administrative effort. You might want to consider performing steps 3 and 4 for one client only, and then copy the keystore file to all other client systems into the same location. With this, all sessions will use the same public key/private key pair.

At this time, the setup is complete. The following steps occur when the secure VT or sftp session is started:

1. The HOD client code uses the JCE to read the public-key from the keystore file.
2. The clients sends its public-key to the SSH server together with a request to authenticate.
3. The SSH daemon (server) reads the public-key from the keystore file, which was transferred in step 4, and checks whether the keys match. If yes, the server returns a packet that indicates that the authentication was successful, and the secure session is established.

Password authentication

Configuring password authentication on the server

The server configuration for password authentication differs depending on the vendor or source of the SSH support. Refer to the documentation for your SSH server software for information on how to configure the SSH server for the password authentication method.

Configuring password authentication on the client

You do not need to configure the client for password authentication. The Host On-Demand client will look for the password in the session configuration information. If no password is found, then Host On-Demand will prompt the user for a password.

For more information, refer to SSH configuration in the online help.

11.5.6 sftp

The sftp (not to be confused with secure FTP which uses TLS/SSL):

- Uses an encrypted connection while (plain) FTP does not
- Runs on a single TCP connection while FTP requires control and data connections
- Has special data structures for getting file list, attributes, etc. while FTP does not have standard way to get file list

11.5.7 SSH trace example

Here is a example of how the started SSH session will appear in a IPMON trace.

Example 11-2 shows the beginning of the SSH session.

Example 11-2 Beginning of the SSH trace

```
[1] 07/27 10:42:01.800 len=22
Outbound:
  5353482D 322E302D 4F70656E 5353485F  <SSH-2.0-OpenSSH_>
  332E3570 310A                        <3.5p1           >

[2] 07/27 10:42:01.820 len=30
Inbound:
  5353482D 322E302D 49424D5F 486F7374  <SSH-2.0-IBM_Host>
  4F6E4465 6D616E64 5F382E30 300A      <OnDemand_8.00   >
```

The server receives a session request on port 22; it sends a version string similar to the above. The string here is SSH, version number, and a comment field. In the comment field, you will usually see the name of the server and its version. The client replies back to the server by sending its own version string. In the case of HOD V8, this is SSH-2.0-IBM_HostOnDemand_8.00.

After exchanging the version string, the server sends the first packet of data. This is not encrypted yet. The first 4 bytes is the length field, indicating the amount of databytes following. In this case x021C = 540 bytes of data. The remainder of the packet are some binary numbers and the list of the encryption algorithms supported by server. See Example 11-3.

Example 11-3   First packet of data from the server

```
[3] 07/27 10:42:01.820 len=544
Outbound:
  0000021C 0914B6B4 FC52B560 3A37B497  <         R `:7  >
  439B8BF2 0E8E0000 003D6469 66666965  <C        =diffie>
  2D68656C 6C6D616E 2D67726F 75702D65  <-hellman-group-e>
  78636861 6E67652D 73686131 2C646966  <xchange-sha1,dif>
  6669652D 68656C6C 6D616E2D 67726F75  <fie-hellman-grou>
  70312D73 68613100 00000F73 73682D72  <p1-sha1    ssh-r>
  73612C73 73682D64 73730000 00666165  <sa,ssh-dss   fae>
  73313238 2D636263 2C336465 732D6362  <s128-cbc,3des-cb>
  632C626C 6F776669 73682D63 62632C63  <c,blowfish-cbc,c>
```

After receiving the list of algorithms from the server, the client sends back its own list of algorithms supported. Again, the first 4 bytes represent the length field. This is shown in Example 11-4.

Example 11-4   Client algorithms sent to server

```
[4] 07/27 10:42:01.850 len=152
Inbound:
  00000094 0A14FCAF 4FCD4E48 DF783C36  <        O NH x<6>
  A3195612 0E320000 001A6469 66666965  <  V  2    diffie>
  2D68656C 6C6D616E 2D67726F 7570312D  <-hellman-group1->
  73686131 00000007 7373682D 64737300  <sha1    ssh-dss >
  00000833 6465732D 63626300 00000833  <   3des-cbc    3>
  6465732D 63626300 00000968 6D61632D  <des-cbc    hmac->
  73686131 00000009 686D6163 2D736861  <sha1    hmac-sha>
  31000000 046E6F6E 65000000 046E6F6E  <1    none    non>
  65000000 00000000 00000000 00000000  <e               >
```

The client then sends some binary data required for starting the encrypted session. Still, this data is not encrypted, and you still see the length field at the beginning of the packet. See Example 11-5.

Example 11-5 Client data to start the encrypted session

```
[5] 07/27 10:42:02.300 len=144
Inbound:
  0000008C 051E0000 008100A0 F7D62AD5  <              * >
  F0C257B7 8DB09E5B 8B050AB5 EE955279  <  W    [      Ry>
  B71233DF D3A34AFD FB266F90 7EDEA185  <  3   J  &o ~   >
  274628CF F5D7C141 689E674C D590E637  <'F(    Ah gL   7>
  363860D7 F6D549D4 DBC26954 7C093ACA  <68`   I   iT| : >
  932FE3EC 269C80C8 FD9BA7DB 3E300F85  < /  &       >0  >
  46DB427F 192D8859 F944AD5A FA4C5FDD  <F B  - Y D Z L_ >
  56842E3F 2B725758 5B3AC0F4 C2144726  <V .?+rWX[:    G&>
  95588097 1EC63EFF 94A94F00 00000000  < X    >   0     >
```

The server replies back to the client. The value *ssh-dss* indicates the DSA algorithm, which will be used for the public key. See Example 11-6.

Example 11-6

```
[6] 07/27 10:42:02.341 len=656
Outbound:
  0000027C 051F0000 01B10000 00077373  <   |          ss>
  682D6473 73000000 8100965E E36C100B  <h-dss      ^ l  >
  F23FAC5A 1C565954 0167B41E 54047657  < ? Z VYT g  T vW>
  89EBBDE9 D93B47B0 8AE01F7C 4BB151C2  <     ;G    |K Q >
  8B6A1198 C2FD1E08 16A9EC9D 37D0D8D7  < j          7   >
  75A1D79F BD1C9849 FD99C323 BD6A4E16  <u      I   # jN >
  D9028770 FA6A2BEE 5F4704BC D7C8048D  <   p j+ _G      >
  9D6CB088 AF6D4B74 A025D5DD A1C0B871  < l   mKt %     q>
  CC7012A4 A1E82B90 DB39D9C7 66C3532B  < p    +  9  f S+>
```

Example 11-7 shows the client's reply. This entry contains actually two packets. The first packet is line 1 of the trace data. The first 4 bytes are still the length field (x0C = 12 bytes). The following x0A is the length of the random padding. The random padding data is at offset 06 to 0F in the first line. Since the packet is not encrypted yet, it contains all nulls. The next byte following is the payload. The x15 means SSH_MSG_NEWKEYS, which indicates that a new encryption key will be used starting with the next packet.

Example 11-7 Client reply to server

```
[7] 07/27 10:42:02.651 len=68
Inbound:
  0000000C 0A150000 00000000 00000000  <                >
  43F3678B 8D6B0B69 E1E66C46 3F33FEAF  <C g  k i  lF?3  >
  F86EBA4E 72868562 C0BE9612 C50B498B  < n Nr  b      I >
  905E7937 7BD57505 BC6908D5 457AD8F9  < ^y7{ u  i  Ez  >
  6D5D1744                             <m] D            >
```

This next packet starts with line 2 of the trace data. As you see the length field at the beginning no longer contains a valid length. The data is encrypted and can no longer be read. After that, all data is fully encrypted. See Example 11-8.

Example 11-8   All data is fully encrypted

```
[8] 07/27 10:42:02.651 len=52
Outbound:
  99E24F04 E2004773 ECC178CC EA7BCE5D  <  O   Gs  x  { ]>
  35862912 EC0F396F F663E203 14B76AEA  <5 )   9o c    j >
  7F1659ED 94C27543 510A27EE F246B232  <  Y   uCQ '  F 2>
  E24DB20A                             < M              >

[9] 07/27 10:42:08.149 len=68
Inbound:
  3F754FA5 BDD18543 3137C4E8 EF760BD8  <?uO    C17   v  >
  ABEAB010 A1ACD372 34556729 F697393F  <       r4Ug)  9?>
```

11.5.8 Should I use SSH, or TLS and SSL?

Both SSH and TLS/SSL provide secure sessions. Which protocol is better for you depends on the characteristics of the system that you support:

- SSH is easier to set up, because it does not require certificates on the client or the host.
- SSH requires the presence of an SSH server on the host.
- Host On-Demand Version 8 supports SSH only on VT and sftp sessions; that is, there is no SSH support on 3270 and 5250 sessions.

11.6 The Host On-Demand Redirector

The Redirector is a Telnet proxy that is written primarily in Java. Refer to 7.3, “Redirector service” on page 339 for a discussion on the Host On-Demand Redirector service. The Redirector is able to accept connections from clients and pass them on, through a different port, to the next stage in the link to the host. The Redirector has the following main functions:

- Hide the real host system address and port number from the client; a common requirement when providing Internet-attached clients access to secure host systems.
- Provide SSL support for all emulator clients when the Redirector is running on Windows NT, 2000 or XP, or AIX.

The Redirector when running on either a Windows NT, WIndows 2000, or AIX server is capable of supporting SSL sessions in one of the following ways:

- Client-side: SSL is enabled between the Redirector and the client.
- Host-side: SSL is enabled between the Redirector and the host Telnet server.
- Both: the Redirector will support SSL sessions on both the client and the host side simultaneously, managing each SSL session separately.

On all platforms the pass-through mode is supported. The pass-through mode allows the client and the server on the other side of the Redirector to communicate in the clear, or to negotiate a secure session directly, including the use of Telnet-negotiated session, basic SSL, and client authentication.

11.6.1 Redirector certificates

When performing SSL, the Host On-Demand Redirector relies on two files for certificate management. These files are found on the Host On-Demand server in the \HostOnDemand\bin directory, and are:

- HODServerKeyDb.kdb

  This is the server's keyring database file, created during SSL configuration (described in 12.3.5, "Create a self-signed certificate" on page 486). It contains:

  - Root certificates for well-known CAs (these are inserted when the file is created)
  - A self-signed certificate (when one exists)
  - Certificates that you have imported from authorities you trust
  - Public keys of all the above certificates
  - Private keys of the self-signed certificate, and of any of your own certificates that have been validated by a CA

- HODServerKeyDb.sth

  This is the password-stash file for the keyring database. It is used to store the password in an encrypted form that can be used by the Redirector to open the keyring database file.

These files are not created at installation. They are created by the certificate management utility when you install the server's certificate, or any unknown CA certificate you may be using.

When using the Redirector and configuring any connection in anything other than pass-through mode, you must install a public key (site) certificate on your server. There are three choices:

- Use a certificate from one of the well-known CAs whose root certificate is already in WellKnownTrustedCAs.class.

- Use a certificate from a CA whose root certificate is not in the file (a unknown CA).
- Use a self-signed certificate.

Obtain a certificate from a certificate authority

To use a certificate from one of the well-known CAs or some other CA, you must request the certificate from the CA, receive the certificate, then store it into the keyring database HODServerKeyDb.kdb file. Nothing else needs to be done to allow the Host On-Demand client to recognize the signer of certificates from the following CAs:

- RSA Data Security, Inc.
- VeriSign, Inc.
- Thawte Consulting

However, if the certificate is from any CA other than one of these well-known CAs that Host On-Demand recognizes, then the public certificate of that signer must be made available to the client in the CustomizedCAs.p12 file. Refer to 12.3.6, “Make a certificate available for the clients” on page 489, and “Using Microsoft cryptographic database” on page 477, or if you are using the Microsoft Internet Explorer 5.0 or above browser, you may authenticate the server’s certificate from the list of CAs that Microsoft recognizes. For the OS/390 server, refer to “Make certificates available to clients” on page 103.

Self-signed certificate

If your security requirements do not warrant the purchase of a commercial certificate; if you need a temporary certificate while you are waiting for your permanent certificate; or if you need one just for testing, you can create your own (self-signed) certificate by using the certificate management utility to create a self-signed certificate. The following is a checklist that can be used to direct your efforts to create and use a self-signed certificate with the HOD Redirector and SSL:

1. Use the certificate management utility to create a new CMS key database file (key database type = CMS, filename = HODServerKeyDb.kdb in \HostOnDemand\bin). Enter a password for the database. Make sure you select **Stash the password to a file**.
2. Select **Personal Certificates** from the drop-down and create a **New Self-Signed Certificate.**
3. Extract the new self-signed certificate as a Base64.arm file to \HostOnDemand\bin. Remember the name of this file.
4. Create a SSLight key database class ((key database type = PKCS12, filename = CustomizedCAs.p12 in \HostOnDemand\HOD). Enter a password for the database.

Important: Make sure, you enter hod as the password. Even if the tool allows you to enter any password you like, HOD will access the database with hod as a hardcoded password.

Select **Signer Certificates** from the drop-down and add the .arm certificate file. Label the certificate appropriately.

5. Save or close the file.
6. Restart the HOD Service Manager.
7. Modify or create a Redirector Service with client-side security.
8. Modify or create a session to connect to the above configured Redirector with SSL enabled.

Refer to 12.3.5, “Create a self-signed certificate” on page 486, or for z/OS, see “Create a self-signed certificate” on page 101.

11.6.2 Configuring the Host On-Demand Redirector

Configuring the Host On-Demand Redirector is covered in 7.3.1, “Configuring the Redirector” on page 340.

11.6.3 Certificate management

For a complete discussion on certificate management, refer to Chapter 12, “Certificate management” on page 473.

11.7 The O/S400 Proxy Server

The OS/400 toolbox delivered the O/S400 Proxy Server to Host On-Demand. The O/S400 Proxy Server is a service that runs on the Host On-Demand server, and provides the ability of a Database On-Demand client and OS/400 file transfer to operate through a single port rather than the standard multiple-port implementation. Refer to Chapter 10, “OS/400 Proxy” on page 397 for details.

11.8 Configuration servlet

Using a configuration servlet allows clients to exchange user authentication and session configuration data over an HTTP(S) connection instead of using the configuration server directly. This eliminates the need to open the configuration server port on the firewall and provides the potential to encrypt all configuration information as it moves from the Web server to the client. For more information regarding configuring the configuration servlet, refer to Chapter 9, “Configuration servlet” on page 387.

11.9 LDAP directory considerations

There are two basic security concerns when using an LDAP security server:

- Securing the communications between Host On-Demand and the LDAP directory server
- Encryption of user passwords within the LDAP directory server

Host On-Demand does not support SSL encrypted communications with the LDAP directory server. All communications will be in the clear; therefore, if you use the LDAP directory server, you may wish to configure the communications link between your Host On-Demand server and the LDAP directory server to occur over a link that resides in the secure network.

Most LDAP directory servers support the storage of user passwords in either clear text, or encrypted. The two most common encryption algorithms implemented are Secure Hash Algorithm (SHA) and UNIX crypt. Some LDAP directory servers now also support MD5. Host On-Demand currently supports passwords stored in clear text, SHA, and UNIX crypt.

11.10 Using Host On-Demand with a firewall

If you are configuring Host On-Demand to go through a firewall, it is recommended that the firewall administrator open only those ports required for the clients to function. At a minimum, you will need to open the following ports:

1. HTTPS port

   This port will be used for downloading the applet and for obtaining configuration information through the configuration server.

2. Telnet ports

   There may be one or more ports open, depending upon the Telnet server requirements. These ports should allow SSL-encrypted session traffic.

3. O/S400 Proxy Server port

   If you are using Database On-Demand or TN5250 file transfer, you should utilize one or more O/S400 Proxy Server ports to pass all traffic over a single port per proxy server.

11.10.1 TCP/IP ports used by Host On-Demand

Table 11-2 identifies all the ports that Host On-Demand will use in its default configuration. Remember that many of the ports are configurable, such as the Service Manager port and the O/S400 Proxy Server port. Use Table 11-2 to determine how to configure your firewall.

Table 11-2 Ports used by Host On-Demand

Host On-Demand Function	Unsecure Port(s) used	Secure Port(s) used
3270 and 5250 Display Emulation	23 (Telnet) 80 (HTTP) 8999 (Service Manager)[3]	992 (Telnet) 443(HTTPS)
3270 and 5250 Printer Emulation	23 (Telnet) 80 (HTTP) 8999 (Service Manager)[3]	992 (Telnet) 443(HTTPS)
3270 File Transfer (IND$FILE)	23 (Telnet) 80 (HTTP)	992 (Telnet) 443(HTTPS)
5250 File Transfer - SAVF file	80 (HTTP) 8999 (Service Manager)[3] 21 (FTP)[4] >1024 (FTP)[4] 446 (drda)[4] 448 (ddm-drda)[4] 449 (as-svrmap)[4] 8470 (as-central)[1 2 4] 8473 (as-file)[1 4] 8475 (as-rmtcmd)[1 4] 8476 (as-signon)[1 4]	443 (HTTPS) 9470 (as-central)[1 2 4] 9473 (as-file)[1 4] 9476 (as-signon)1 4
5250 File Transfer - database	80 (HTTP) 8999 (Service Manager)[3] 446 (drda)[4] 448 (ddm-drda)[4] 449 (as-svrmap)[4] 8470 (as-central)[1 2 4] 8473 (as-file)[1 4] 8475 (as-rmtcmd)[1 4] 8476 (as-signon)[1 4]	443 (HTTPS) 9470 (as-central)[1 2 4] 9473 (as-file)[1 4] 9476 (as-signon)1 4
5250 File Transfer - stream file	80 (HTTP) 8999 (config server)[1 2 4] 448 (ddm-drda)[4] 449 (as-svrmap)[4] 8470 (as-central)[1 2 4] 8473 (as-file)[1 4] 8476 (as-signon)1 4	443 (HTTPS) 9470 (as-central)[1 2 4] 9473 (as-file)[1 4] 9476 (as-signon)1 4
Host On-Demand Administration	80 (HTTP) 8999 (Service Manager)[3]	443 (HTTPS)

Host On-Demand Function	Unsecure Port(s) used	Secure Port(s) used
Database On-Demand	80 (HTTP) 8999 (Service Manager)[3] 448 (ddm-drda)[4] 449 (as-svrmap) [4] 8470 (as-central)[1 2 4] 8471 (as-database)[1 4] 8476 (as-signon)[1 4]	443 (HTTPS) 9470 (as-central)[1 2 4] 9476 (as-signon)1 4
License Use Count	8999 (Service Manager)[3] 80 (HTTP)	8999 (Service Manager)[3] 443 (HTTPS)

Notes: Port numbers listed are the default values.
[1]You can change the port numbers with the OS/400 WRKSRVTBLE command. The port numbers listed are the default values.
[2]The port for as-central is used only if a code-page conversion table needs to be created dynamically (EBCDIC to/from unicode). This is dependent on the JVM and the locale of the client.
[3]You can change the Service Manager port.
[4]These ports do not need to be opened on the firewall if you are using O/S400 Proxy Server support. You will need to open the default proxy server port 3470. You can change this port.

11.11 Native Authentication

User ID and password management has become an ever-increasing issue for users as the number of systems, and applications that require authentication continues to grow. In order to save a user's preferences at the Host On-Demand server, a user ID is required to uniquely identify the user. This ID is used as the index under which the user's preferences are stored in the repository. Host On-Demand does not require passwords to be implemented with the user ID; however, most customers implement a password for an additional level of identification. Because of the platform-independent nature of Host On-Demand, this user ID and password management as implemented by Host On-Demand is independent of any other user ID and password management system.

Host On-Demand requires the administrator to define and manage user IDs when a configuration server model is implemented, but with the introduction of the Native Authentication component we allow the administrator to associate the Host On-Demand user ID with a user ID and password known to the native operating system. The native platform authentication service allows users to log on to Host On-Demand using the same password as they would to log on to the operating system where Host On-Demand is active (Windows NT Server, AIX, or z/OS). When a user logs on to Host On-Demand, their password is validated against the system password, rather than a separate Host On-Demand password, thus providing the customer with the following benefits:

- Reducing the number of passwords that the end user must remember. In many cases this means that the user will have only one password to remember.
- Better security, and a reduction in the administrative workload for the Host On-Demand administrator by delegating password management to an administrative system that can implement a password management policy that typically includes:
  - Enforcement of password rules
  - Enforcement of password expiration times
  - Ability to revoke access by invalidating a password

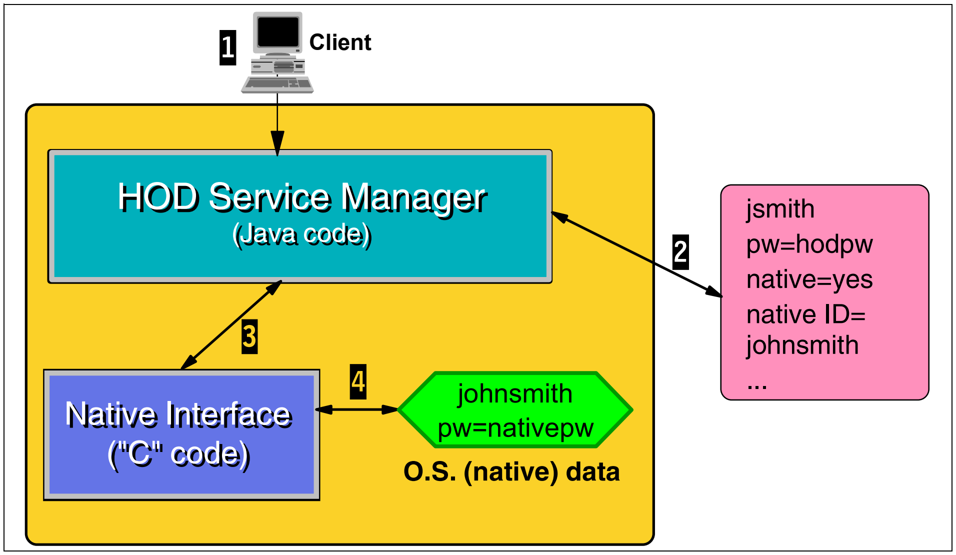


Figure 11-25 Native Authentication login flow

When a user logs on (**1**), the user ID and password are sent to the Host On-Demand configuration server. The configuration server sends a request for logon information about the user to the LDAP server (**2**). The LDAP server returns a message indicating if the user is configured for Native Authentication. If the user is not configured for Native Authentication, the password stored in the LDAP directory server is returned to the configuration server. If the user is configured for Native Authentication, the native ID stored in the LDAP directory is returned along with an indicator that Native Authentication should be invoked. The configuration server checks the returning information from the LDAP directory server. If the user is configured to use Native Authentication, the configuration server sends the user ID and the password to be authenticated to a Host On-Demand module written in C,and compiled for the specific operating system (**3**). That module will invoke the appropriate native operating system security call to validate the user ID and password combination (**4**). If the user is not configured for Native Authentication, the configuration server compares the password that was entered by the user with the password returned by the LDAP server.

If the user ID and password are successfully validated by the operating system, processing continues. All other returns will result in an invalid password error message as shown in Figure 11-26. Other than a legitimately invalid password, one of the most common reasons for this return message will be an expired password. There is no mechanism within Host On-Demand to intercept an expired password and prompt for a new one. The user will be required to correct this condition through some other interface, and then log on again to Host On-Demand.

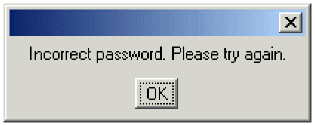

Incorrect password. Please try again.

Figure 11-26 Native Authentication failure

11.11.1 Native platform authentication requirements

Native platform authentication service must be installed on a Windows NT, Windows 2000, AIX, or zSeries Host On-Demand server. On Windows NT or 2000 native platform authentication requires a Windows NT server or Windows Advanced NT server (LANMAN) with a non-null domain.

On the Host On-Demand server, LDAP directory services must be enabled and configured for Native Authentication individually for each user that is to use Native Authentication; refer to 7.1.4, “Using Native Authentication” on page 273. The LDAP directory server may reside anywhere in the network, and may run on any platform.

Follow the steps below to use native platform authentication with Host On-Demand:

1. Enable users for Native Authentication.
2. Start the native platform authentication service.
3. Configure current users for Native Authentication.

11.11.2 Installation and activation

The files to support native platform authentication are installed with the Host On-Demand server during the installation process. With Windows NT and Windows 2000, some additional installation steps are required as defined below.

Windows NT and Windows 2000

The operating system must be Windows NT server, Windows 2000 server, or LANMAN.

On Windows NT and Windows 2000, Native Authentication runs as a service: the IBM ODS Platform Authentication Service.

Update the registry

On Windows NT and Windows 2000, the following additional steps are required to update the registry:

1. Define a new environment variable, hod_dir, and set its value to the drive letter where Host On-Demand is installed. The hod_dir environment variable is used by the registry settings to locate Host On-Demand. To update the variable, click **Start -> Settings -> System**, select the **Environment** tab, and add a system variable hod_dir=x:, where x is the drive where Host On-Demand is installed. It must be a system variable, not a user variable, so that the services can use it.
2. Using Windows NT Explorer, locate the odsrapd.reg file in the Host On-Demand bin directory, and double-click the file to add the registry settings defined in the file.

> **Important:** There will be two ODSRAPD files: ODSRAPD.EXE and ODSRAPD.REG. Make sure you are selecting the odsrapd.reg file verifying that the type attribute is Registration Entries not Application.

3. This step is only required for Windows NT; it is not required for Windows 2000. Using **`regedit`**, find the registry value for:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\IBM\On-Demand Server for Windows
   NT\2.0\installpath
   ```

   Edit the installpath value so that `%hod_dir%` is replaced with the drive letter where Host On-Demand is installed. For example, if Host On-Demand is installed on the D drive, change:

   ```
   %hod_dir%\HostOnDemand\private
   ```

   to

   ```
   d:\HostOnDemand\private
   ```

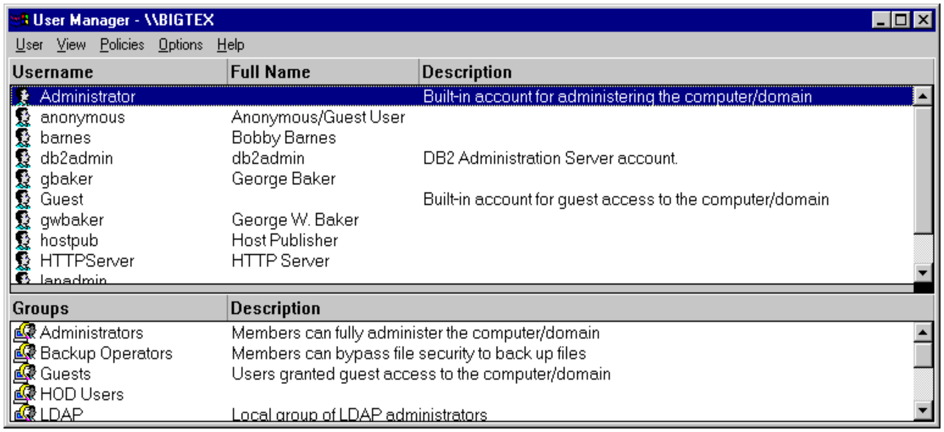
4. Reboot the server.

Once you reboot, you can go to the Services window by clicking **Start -> Settings -> Services**, and you should see IBM ODS Platform Authentication Service showing as started.

Set user rights policies

The final step is to set the proper user rights in the Policies section of the User Manager. To set the correct user rights in the Windows NT system, follow these instructions:

1. Open the User Manager on Windows NT. This is normally found by clicking **Start -> Programs -> Administrative Tools (Common) -> User Manager**.

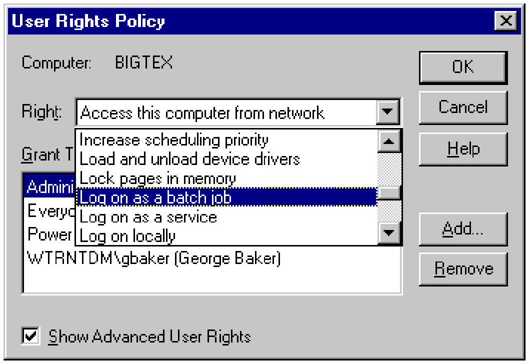


Username	Full Name	Description
Administrator		Built-in account for administering the computer/domain
anonymous	Anonymous/Guest User	
barnes	Bobby Barnes	
db2admin	db2admin	DB2 Administration Server account.
gbaker	George Baker	
Guest		Built-in account for guest access to the computer/domain
gwbaker	George W. Baker	
hostpub	Host Publisher	
HTTPServer	HTTP Server	
lanadmin		

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
HOD Users	
LDAP	Local group of LDAP administrators

Figure 11-27 Windows NT User Manager

2. Click **Policies** > **User Rights** from the menu bar of the User Manager.
3. Check **Show Advanced User Rights**.
4. In the Right field, select **Log on as a batch job**. See Figure 11-28.



Computer: BIGTEX

Right: Access this computer from network

Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Log on as a service
Log on locally

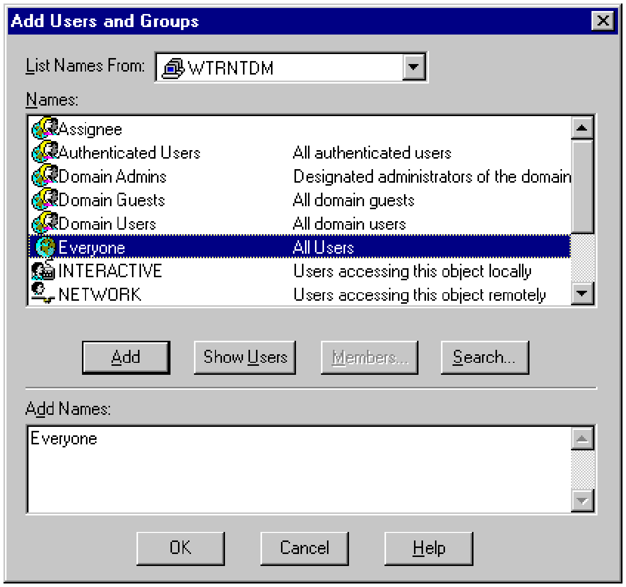
Grant T

Admini
Everyo
Power
WTRNTDM\gbaker (George Baker)

☑ Show Advanced User Rights

Figure 11-28 Advanced user rights

5. Click **Add**.
6. From the Names field, select users who will be using native platform authentication and click **Add**. To add members of a group, select the group and click **Members**. As you add users, the users' names are displayed in the Add Names field. We recommend that you either allow the group of all users, Everyone, or create a group, such as Host On-Demand, and include all Host On-Demand users in this group.



List Names From: WTRNTDM

Names:

Assignee	
Authenticated Users	All authenticated users
Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Everyone	All Users
INTERACTIVE	Users accessing this object locally
NETWORK	Users accessing this object remotely

Add Names:

Everyone

Figure 11-29 Adding authorized users

7. When you are finished adding users, click **OK** to close the Add Users and Groups window, and save your changes.
8. Click **OK** to close the User Rights Policy window.

You can now exit the User Manager. All users that were granted the right to log on as a batch job can be authenticated using the native platform authentication service.

The native platform authentication service is started from the Windows NT Services menu. By default, this service is set to start automatically.

zSeries

For information on zSeries support for Native Authentication, refer to 3.9, “Native Authentication” on page 123.

AIX

To start the program, a user with root authority must execute the shell script `odsrapd.sh`, which is located in the /usr/opt/HostOnDemand/bin directory.

The syntax for the start is as follows:

```
odsrapd.sh [parameters]
```

Where the parameters are as follows:

-l Enables logging. You can also specify `-L`, `/l`, or `/L`. Note: Native Authentication code logs its messages to the syslog, which may need to be configured to log the desired level of messages.

-txx Sets the socket timeout to some other value instead of the default 20 seconds. You can also specify `-T`, `/t`, or `/T. xx` as the new timeout value.

-cxx Specifies the number of requests the server will allow. You can also specify `-C`, `/c`, or `/C. xx` as the new number of requests the server will handle.

The Native Authentication code uses the syslog to log its messages. If you do not already have one defined, you may need to configure one in order to log the desired level of messages. One of the key prerequisites is that the log must exist prior to `odsrapd` trying to access it.

The syslog can be configured to report any level of message desired, but initially it is best to get all levels (debug). Once everything is working well, you can restrict the message reporting to just errors (crit). Modifying syslog information will require root authority.

Adding the following line to the end of the /etc/syslog.conf file will log all messages to /etc/hod/rapd.out:

```
user.debug/etc/hod/rapd.out
```

The syslog daemon will not log the messages if the file does not exist; therefore, you must create the rapd.out, if it does not already exist. Finally, stop and restart syslogd so that it reads its new configuration file.

Before you run the shell script for the first time, you will need to change the permissions on both the **odsrapd.sh** shell script and the **odsrapd** executable. You should verify that the Native Authentication code started correctly by checking the syslog for a starting message from **odsrapd**. This message will be in the file rapd.out if you used the sample provided here.

11.11.3 Debug information

If you have problems getting Native Authentication working, you will need the following information to assist in debugging the problem:

- System type
- User's Host On-Demand and native user IDs
- User's error message
- Host On-Demand Service Manager trace with level 3 debug messages
- Native Authentication logged messages (syslog messages on AIX and zSeries), or the event viewer application log for Windows NT and Windows 2000

11.12 Integrated Windows domain logon

Access to information is becoming increasingly complicated in terms of security. Every user is expected to pass through several layers of security measures before they actually access the information. This could start with a power-on password, and proceeds through several layers of network and application security. This leads to complex security layers and administration policies. The IBM Host On-Demand Integrated Windows domain logon feature is here to reduce the complexity by at least one layer without any compromise to the security.

The Integrated Windows domain logon feature is a feature available to Host On-Demand V6.0 and later Windows users only, and is only valid for Configuration Server-based model users, where users are required to log on to the Host On-Demand server to obtain their session preferences. Enabling this function causes the Host On-Demand client to query the Windows operating system, and retrieve the domain and user ID used during Windows logon. The returned user ID then becomes the Host On-Demand user name. The domain returned will be compared to the list of allowed domains for the users, and if valid, will invoke the login process with the configuration server automatically without prompting the user.

The benefits of using this feature are:

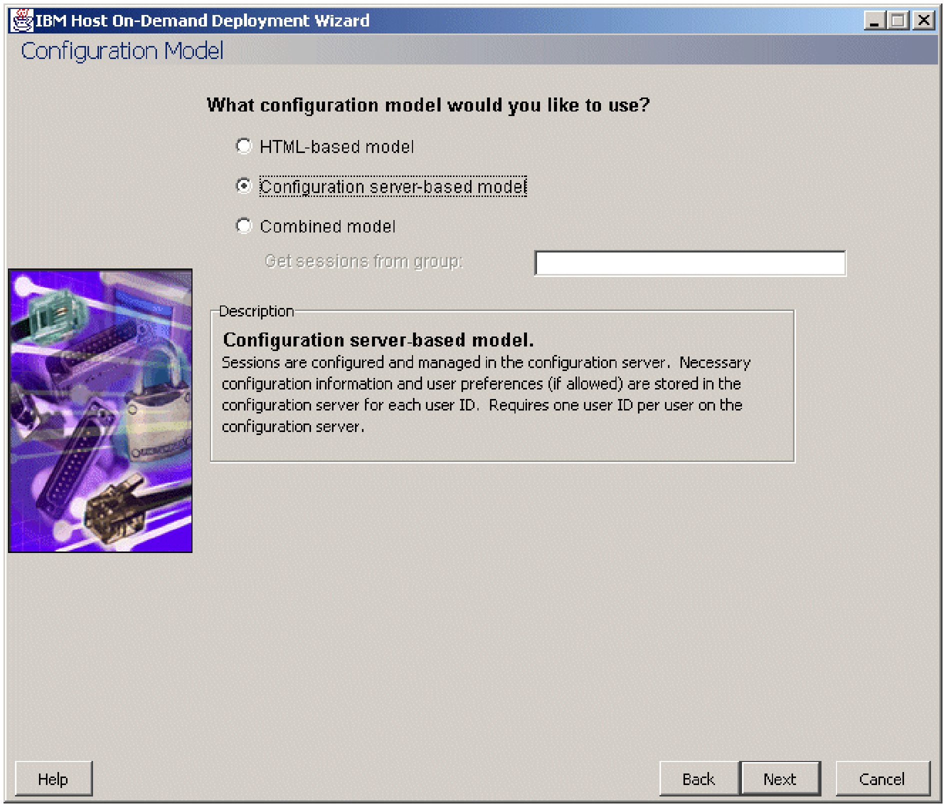
- A reduction in the number of user IDs and passwords the user has to remember.
- Security and password management is done by the Windows workstation and the domain controller.
- Reduces the administrative workload on the Host On-Demand administrator, since the administrator need not create and maintain individual user IDs.
- Users will bypass the Host On-Demand logon window.

The Host On-Demand server may be on any platform, since all Integrated Windows domain logon service functions are performed on the Windows client. For Integrated Windows domain logon to work, the user must invoke the Host On-Demand using an HTML file that has been specifically created with the Deployment Wizard by the administrator. See 11.12.1, “Activating Integrated Windows domain logon” on page 461.

11.12.1 Activating Integrated Windows domain logon

The following steps must be performed by the administrator in order to enable Integrated Windows domain logon:

1. Start the Host On-Demand Deployment Wizard (for details, see 14.2, “Starting the Deployment Wizard” on page 518).
2. In the first window, select **Create an HTML file** and click **Next** to display the window shown in Figure 11-30.



What configuration model would you like to use?

○ HTML-based model

● Configuration server-based model

○ Combined model

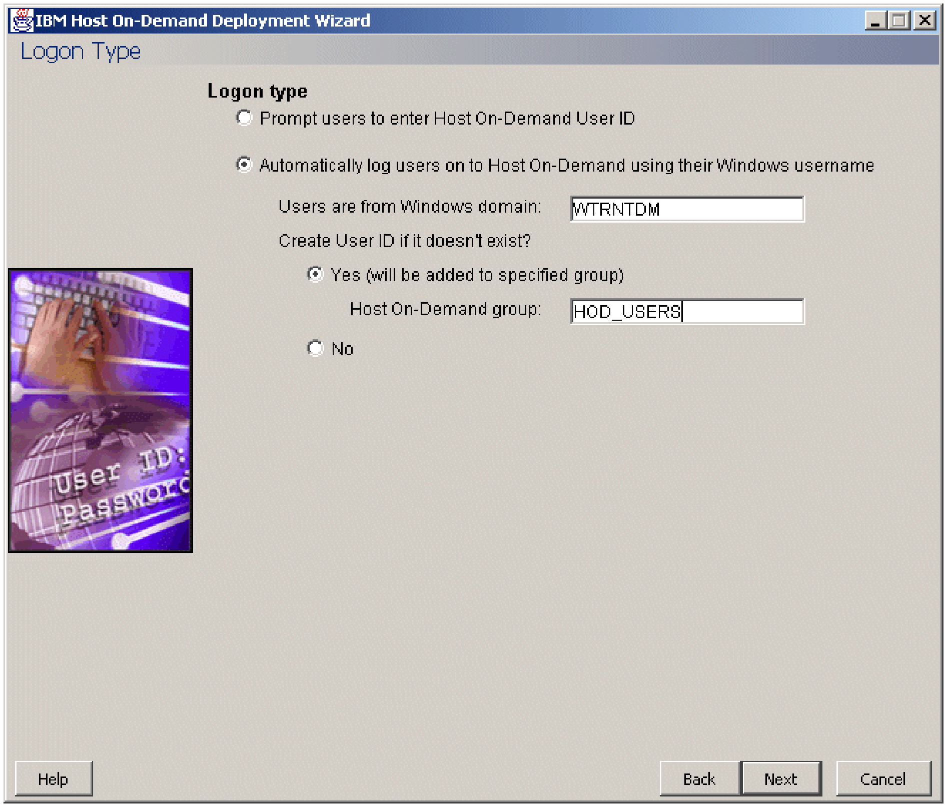
Get sessions from group:

Description

Configuration server-based model.
Sessions are configured and managed in the configuration server. Necessary configuration information and user preferences (if allowed) are stored in the configuration server for each user ID. Requires one user ID per user on the configuration server.

Figure 11-30 Configuration server based model

3. Select **Configuration Server-based model,** then click **Next** to display the panel shown in Figure 11-31.



Logon type

○ Prompt users to enter Host On-Demand User ID

● Automatically log users on to Host On-Demand using their Windows username

Users are from Windows domain: WTRNTDM

Create User ID if it doesn't exist?

● Yes (will be added to specified group)

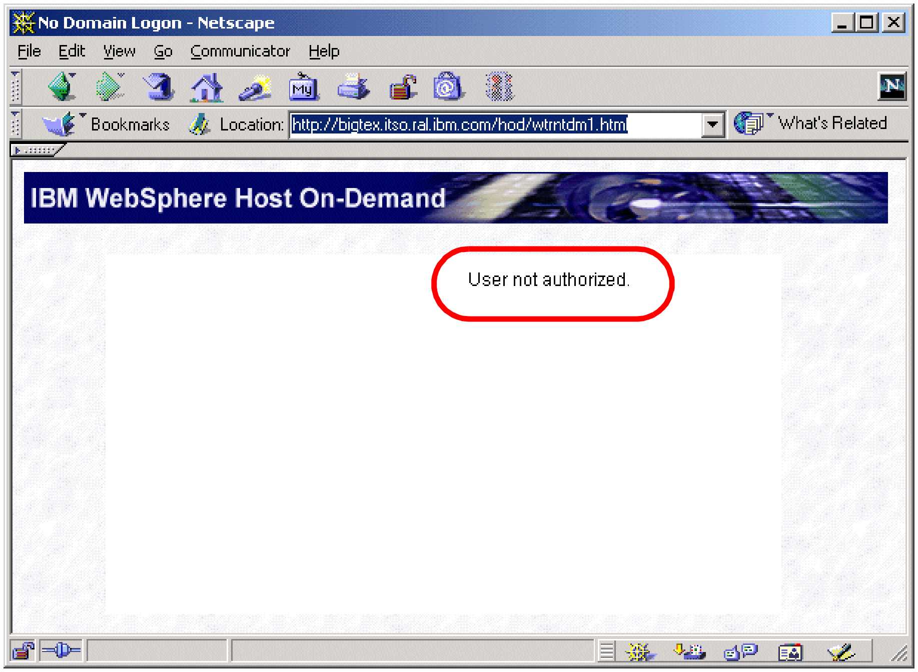
Host On-Demand group: HOD_USERS

○ No

Figure 11-31 Single sign-on option selected

4. Select **Automatically Log users on to the Host On-Demand using Windows username**.

5. This will enable the options previously greyed out. In the first field enter the domain or domains, separated by a comma, into which the user must log on. If the user is not logged into one of these domains, the user will be presented with a message that they are not authorized as shown in Figure 11-32.


No Domain Logon - Netscape
File Edit View Go Communicator Help
Bookmarks
Location:
http://bigtex.itso.ral.ibm.com/hod/wtrntdm1.html
What's Related
IBM WebSphere Host On-Demand

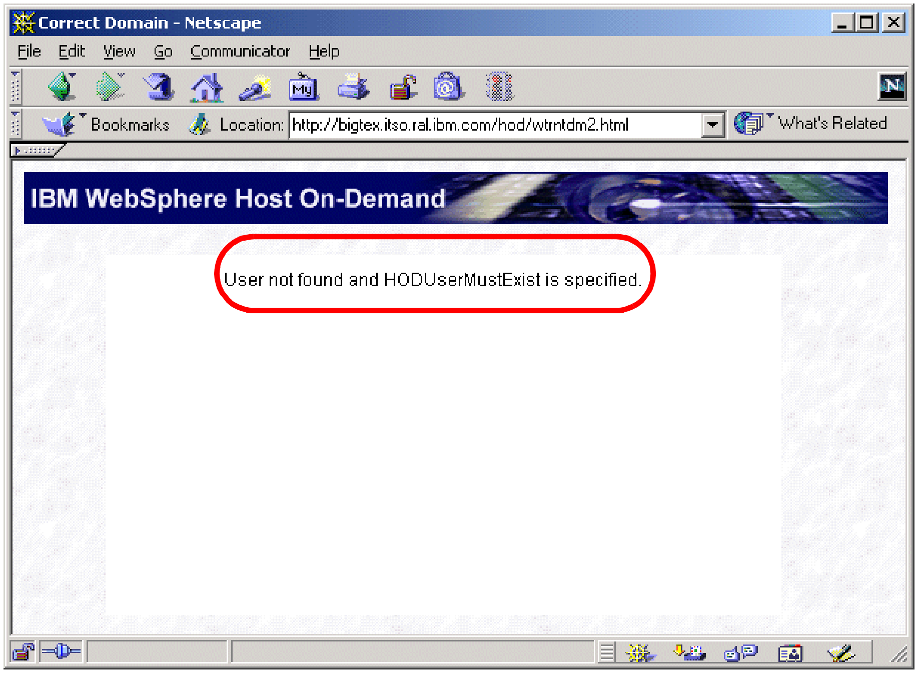
User not authorized.

Figure 11-32 Integrated sign-on - not authorized

6. Next, you must indicate if the configuration server is to create the user ID for the incoming user ID. Does it or does it not pre-exist?

   a. Selecting **Yes** results in the specified user ID being created in the group specified in the following field.

b. Selecting **No** results in a message that the user does not exist, and the logon is denied since the user was not predefined (see Figure 11-33).



Correct Domain - Netscape
File Edit View Go Communicator Help
Bookmarks
Location: http://bigtex.itso.ral.ibm.com/hod/wtmtdm2.html
What's Related
IBM WebSphere Host On-Demand

User not found and HODUserMustExist is specified.

Figure 11-33 User not found

7. Specify the Host On-Demand group in which new users will be created. If this field is left blank, the user will be added to the `HOD` default group. If specified, the group must already exist.

> **Note:** Host On-Demand will insert `Created by System` into the description field of the user record.

8. Click **Next** to proceed through the remainder of the Deployment Wizard as documented in Chapter 14, “Deployment Wizard” on page 517 to complete the configuration, store, and activate the HTML file.
9. Inform the users of the existence of this HTML file.

11.12.2 Process flow

Figure 11-34 illustrates how this process works.

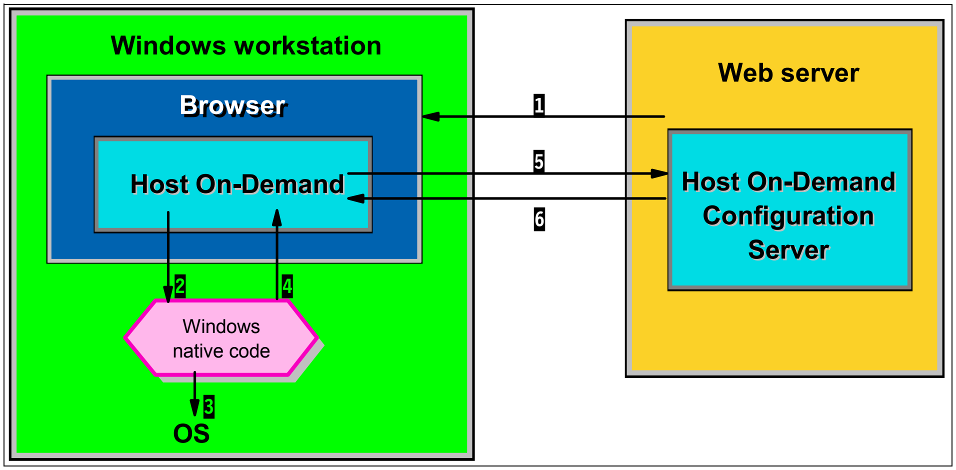


Figure 11-34 Integrated Windows domain logon flow

Here are the steps:

1. The user downloads Host On-Demand client into the browser using an HTML file created by the administrator with the Deployment Wizard.
2. When the Host On-Demand client detects that Integrated Windows domain logon has been enabled, a call is made to the native Windows code.
3. The native Windows code queries the operating system to obtain the user ID and domain specified during user logon. If the user performed a local logon, the domain to which the system is defined will be returned.
4. The native code returns the user ID and domain name to the Host On-Demand client.
5. The domain name is compared to the list of domain names specified by the administrator. If the domain name does not match the request, it is rejected and the user notified as shown in Figure 11-32 on page 464.
6. If there is a domain name match, then the configuration server is contacted to obtain the user preferences. The process will create the user not already present.

11.12.3 Configuration parameters

The following are the parameters generated and stored in the params.txt file by the Deployment Wizard when Integrated Windows domain Logon is specified.

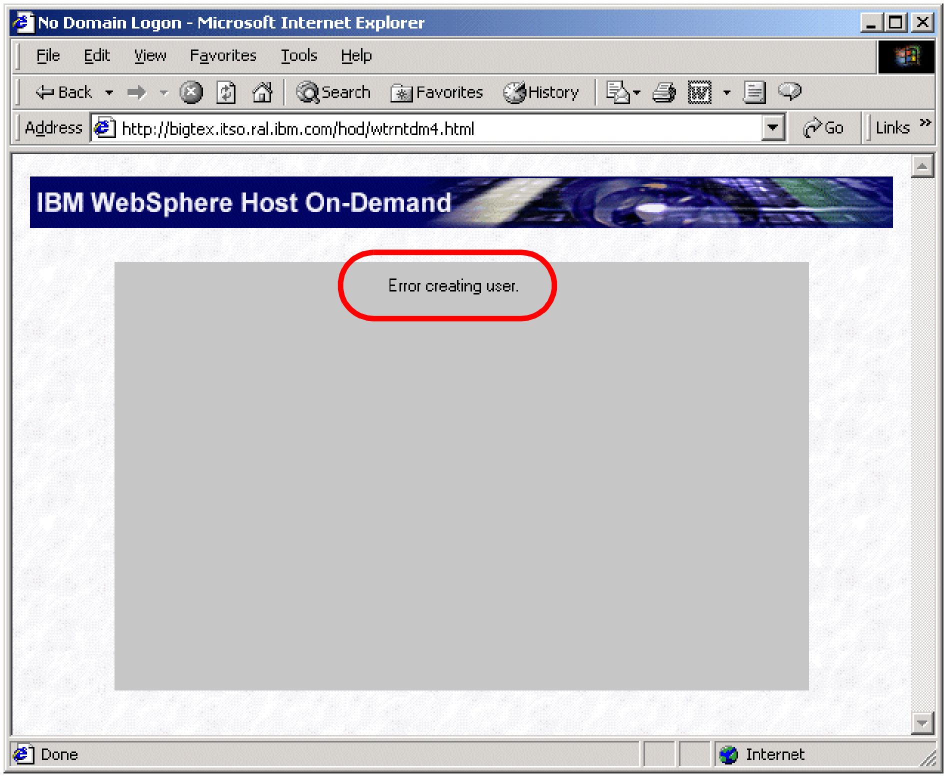
Table 11-3 Integrated Windows domain logon parameters

Parameter	Value
UseWindowsDomain	True if this feature is enabled, else false
WindowsDomain	A comma separated list of authorized domains
HODUserMustExist	True, or false if the user may be automatically added if it does not exist
WDHODGroup	Group name to be used if HODUserMustExist=false

11.12.4 Troubleshooting

Be aware of the following issues:

- Invalid information specified such as the Host On-Demand group in which the user IDs are to be automatically created. This results in the error are shown in Figure 11-35.


No Domain Logon - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://bigtex.itso.ral.ibm.com/hod/wtrntdm4.html
Go Links
IBM WebSphere Host On-Demand
Done
Internet

Error creating user.

Figure 11-35 Invalid group

- If the user loads any Host On-Demand HTML file that is configured for the configuration server model that was not enabled for the Integrated Windows domain logon feature, the user will be prompted for a user ID and password.

> **Important:** The user will be prompted in this environment because the system assigned a random password when his user ID was automatically created. To log on conventionally, the user must have this password reset by the administrator.

11.13 Telnet-negotiated session

The purpose of Telnet-negotiated session is to allow a Telnet session to begin as a non-secure session, but then negotiate a secure session over a Telnet connection using the Transport Layer Security (TLS) handshake protocol.

The TLS protocol is defined in IETF Standards Track RFC 2246 “The TLS Protocol 1.0” and is found at:

```
http://www.ietf.org/rfc/rfc2246.txt
```

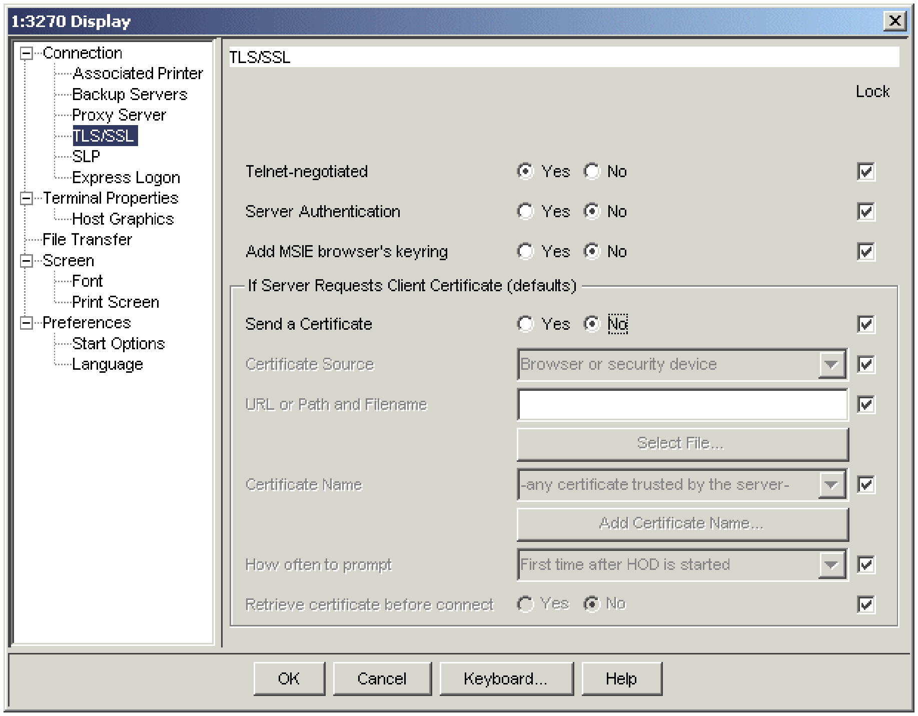
Host On-Demand V8 includes native support for Transport Layer Security protocol V1.0. It allows for negotiation down to SSL for those servers that have not yet implemented support for TLS. The TLS protocol syntax and handshake flow remains virtually unchanged from those of SSL. The significant difference is that the hello message for TLS must contain Version 3.1. Once it has been agreed by both client and server that 3.1 is to be used, cipher suite exchanges will use a prefix of `TLS_` instead of the SSL 3.0 prefix of `SSL_`.

Enhancements from SSL V3.0 to TLS V1.0 include:

- Additions to the number of “alert” messages defined in the protocol
- Standardized method of calculating message authentication codes (MAC)
- Simplified CertificateCertify message

11.13.1 Session configuration

In order to implement Telnet-negotiated security, you must first select either **Telnet - TLS** or T**elnet - SSL only** as the protocol on the Connection window, then select **Yes** to the Telnet-negotiated radio button (see Figure 11-36).



TLS/SSL

Lock

Telnet-negotiated ● Yes ○ No ☑

Server Authentication ○ Yes ● No ☑

Add MSIE browser's keyring ○ Yes ● No ☑

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No ☑

Certificate Source: Browser or security device ☑

URL or Path and Filename ☑

Select File...

Certificate Name: -any certificate trusted by the server- ☑

Add Certificate Name...

How often to prompt: First time after HOD is started ☑

Retrieve certificate before connect ○ Yes ● No ☑

Figure 11-36 Enable TLS-negotiated security

The other security options are valid regardless of whether the Telnet-negotiated radio button is Yes or No. Selecting Telnet-negotiated determines if the TLS/SSL negotiation between the client and the server is done on the Telnet connection, or on a TLS/SSL connection prior to the Telnet negotiations. Selecting **No** forces a secure session before initiating the Telnet session.

If **Yes** is selected for Telnet-negotiated, then the Telnet protocol will be used to negotiate the TLS/SSL security after the Telnet connection is established. This support is applicable only with a Telnet server that supports Telnet-negotiated sessions. CS for OS/390 V2R10 and z/OS are the only IBM Telnet Servers at this time that support this function.

If **No** is selected for Telnet-negotiated, the traditional TLS/SSL negotiations will be done on a TLS or SSL connection with the server, and subsequently the Telnet negotiations with the server will be done. The default is No because few Telnet servers have this support.

Please note that the settings on the TLS/SSL selection are only in effect when the protocol on the Connection selection has been set to either **Telnet - TLS** or **Telnet - SSL only**. Otherwise, regardless of the settings on the TLS/SSL selection, the session will have *no* security at all.

If security is disabled, and the server requests a Telnet-negotiated secure session from the client, the Host On-Demand client will not start a session, and an error message will be issued.

The CS for OS/390 documentation refers to this feature as “negotiable SSL.”

11.13.2 Session negotiation

A typical Telnet-negotiated SSL flow is shown in Figure 11-37.

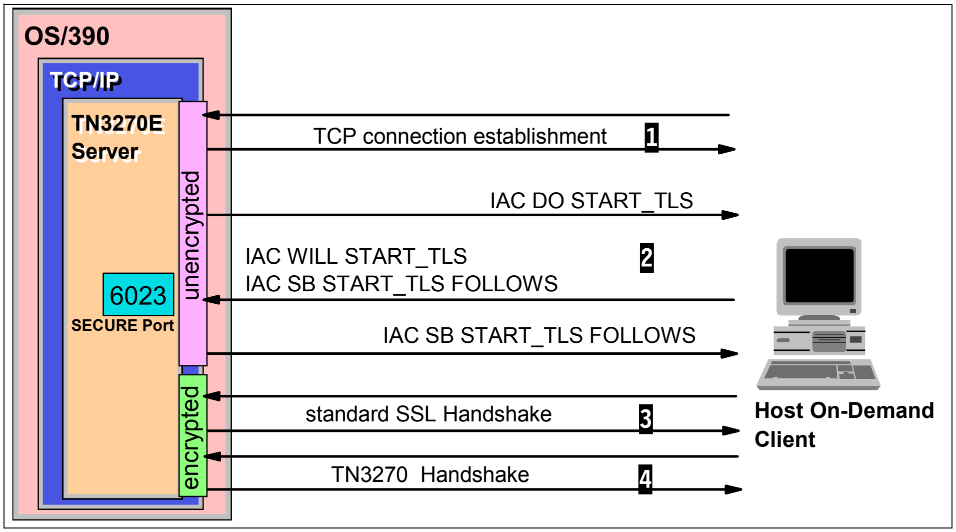


Figure 11-37 TLS-based Telnet SSL flow

Here are the steps:

1. IP connection establishment
2. The Telnet server sends the **`IAC DO START_TLS`** command to the client to verify if it wants to perform the SSL negotiation.
3. If a positive response is received, then Telnet begins a normal SSL handshake.
4. If no positive response is received, the connection will be dropped.

The **`IAC DO START_TLS`** Telnet command, sent from the server, activates TLS at the beginning of a Telnet connection. The client can respond to this command by sending the **`IAC WILL START_TLS`** command, if the negotiation of a TLS connection is required. With the **`IAC DONT START_TLS`** command, the client can refuse the TLS connection negotiation. Sending the **`IAC SB START_TLS FOLLOWS IAC SE`** command initiates a TLS negotiation. When this subcommand has been sent and received, the TLS negotiation will begin.

If security is enabled and Telnet-negotiated is `Yes`, then the Telnet connection will be started normally without SSL. However, the 3270 session will not start until the SSL negotiation completes successfully. If the server responds with the message `WONT STARTTLS`, then the session will not start, and an error message will be issued stating: `Security was requested, but the server does not support security`.

If security is disabled and the server requests a TLS session, Host On-Demand will not start a TLS session, and an error message will be displayed on the status bar stating: `The server requested security, but Security is not enabled.`

12

Certificate management

Certificate management is central to the operation of SSL. This chapter identifies the critical Host On-Demand files that you must be aware of when managing certificates. We then discuss the impacts of using certificates from different sources, such as well-known Certificate Authorities (CAs), unknown CAs, and self-signed certificates, and how to deploy server certificates to the clients.

Finally, we discuss the utilities available for creating and managing certificates:

- The certificate management utility
- The IKEYCMD command-line tool
- The keyring utility

Note that the Certificate Wizard available in previous releases of Host On-Demand has been removed in Host On-Demand V8.

12.1 Files managed by certificate management

The Host On-Demand Redirector uses the files for key and certificate management on the Host On-Demand server. These files are kept in \HostOnDemand\bin, and are:

- HODServerKeyDb.kdb, the server's keyring database file. It contains:
  - Root certificates for well-known Certificate Authorities (CAs) (these are inserted when the file is created).
  - Self-signed certificates (if they exist).
  - Certificates that you have imported from authorities you trust.
  - Public keys of all the above certificates.
  - Private keys of the self-signed certificate, and of any of your own certificates that have been validated by a CA.
- HODServerKeyDb.sth, the password stash file for the keyring database is used to store the password in an encrypted form that can be used by the Redirector and/or the Express Server to open the keyring database file.

These files are not created at installation. You must create them by means of the certificate management utility.

Download and locally installed clients use the Java classes WellKnownTrustedCAs.class and CustomizedCAs.p12 to perform authentication. With download clients (including cached clients), these are downloaded from the server as required. Locally installed clients use their locally held copies. The CustomizedCAs.p12 is created or updated by the Certificate Management Utility during SSL configuration; it contains the server and CA-root certificates. It must be updated whenever a self-signed certificate is introduced or a certificate from an authority other than one of those well-known CAs is to be used. To be accessible to download clients, both classes are stored in the publish directory.

12.2 Using certificates

To enable SSL for your Redirector, you must install a public key (site) certificate on your server. There are three choices:

1. Use a certificate from one of the well-known CAs whose root certificate is already in the `WellKnownTrustedCAs.class`:
   - RSA Data Security, Inc.
   - VeriSign, Inc.

- Thawte Consulting

2. Use a certificate from a CA whose root certificate is not in the file (an unknown CA).

   There are many well-known Certificate Authorities that are not in the WellKnownTrustedCAs.class file that you use as your CA, because they are not listed in the WellKnownTrustedCAs.class file, where they will be referred to as unknown CAs.

3. Use a self-signed certificate.

The tool that allows you to manage all these certificates is explained in 12.3, “Certificate management utility” on page 478.

You can send certificate requests to the following companies, which already have their public keys recognized by Host On-Demand:

```
http://www.verisign.com
http://www.thawte.com
```

12.2.1 Using a site certificate from a well-known CA

To use a certificate from one of the well-known CAs, you must obtain it from the CA, and add it to HODServerKeyDb.kdb on the server. All clients will recognize it and authenticate with it. The steps are:

1. Create the certificate request.
2. Submit the certificate request to the CA.
3. Obtain and store the certificate in the server’s keyring database.

Public key certificates of well-known CAs

The public key certificates (or root certificates) of a number of well-known CAs are automatically inserted into the keyring databases when they are created. Their names are displayed by the certificate management utility, as shown in Figure 12-9 on page 487.

12.2.2 Using a certificate from an unknown CA

If you wish to use a certificate from an unknown CA, the procedure is more complicated. The steps are:

1. Create the public-key/private-key pair and the certificate request.
2. Submit the certificate request to the CA.
3. Obtain the certificate from the CA.
4. Obtain the CA’s root certificate and store it in the keyring database.
5. Store the site certificate in the keyring database.

6. For downloaded clients, use the key management utility to add the formatted CA root certificate to the `CustomizedCAs.p12` on the server. Refer to 12.3.6, “Make a certificate available for the clients” on page 489.
7. For locally installed clients, extract the certificate from the server’s keyring database file, take or send the certificate to the client through a secure mechanism, and add it to the client’s keyring database file.

12.2.3 Using a self-signed certificate

SSL can be set up quickly and easily to use a self-signed certificate. This is useful for testing purposes or while waiting for a certificate from an unknown CA. It should not be used in a production environment.

The steps are:

1. Using the certificate management utility, create a self-signed certificate. A public-key and private-key pair and a certificate are automatically created. Then store these into the keyring database.
2. For all Host On-Demand clients, except a locally installed client, extract the self-signed certificate from the database to the `CustomizedCAs.p12.`
3. For locally installed clients, extract the certificate from the server’s keyring database file, take it to the client and add it to the client’s keyring database file.

12.2.4 Making server certificates available to clients

All clients must be able to authenticate the signer of the server certificate. If the signer exists in the WellKnownTrustedCAs.class file, nothing more needs to be done, since all Host On-Demand clients on all platforms have access to this file either locally installed or downloaded from the server.

If you use a certificate from a CA that is not contained in the Host On-Demand WellKnownTrustedCAs.class file, or you use a self-signed certificate, you must provide the client with the signer’s public certificate.

The traditional method is to add the signer certificate to the CustomizedCAs.p12 file. Download clients receive this file from the server when they load the applet, while locally installed clients must have this file either created or installed on each client separately.

Beginning with Host On-Demand Version 5.03, there is another method for Windows platform users: the Microsoft cryptographic database, which contains many more signer certificates than does the WellKnownTrustedCAs.class file.

Downloaded and cached clients

Downloaded and cached clients must be able to access the certificate from the Host On-Demand server. If the server is using a certificate from a well-known CA, nothing more needs to be done because the certificate is already in the WellKnownTrustedCAs.class file in the “publish” directory, and is therefore accessible to clients. However, if the certificate is self-signed or from an unknown CA, it must be put into the CustomizedCAs.p12 file, which must be present in the “published” directory.

The CustomizedCAs.p12 file is always downloaded to all download clients and available for use even if they are configured to use the cryptographic database. This insures that all clients will have the certificate when required regardless of platform.

Locally installed clients

There are two ways to enable a locally installed client to recognize certificates signed by unknown CAs:

- Build the CustomizedCAs.p12 file at the central site and transfer it to the client through a secure method that meets your security policy. The user need only store it in the \HostOnDemand\lib subdirectory of his system to make it available.
- Update the locally installed client on the workstation. The administrator must transfer the binary DER file of the certificate to each user that has a locally installed client. The user of that machine must then run the Certificate Management Utility from the local Host On-Demand installation. For security purposes, it is recommended that the binary DER file and the password be sent through separate out-of-band methods.

Using Microsoft cryptographic database

The Microsoft cryptographic database contains a much larger list of recognized CAs than does the Host On-Demand WellKnownTrustedCAs.class file. You may use this cryptographic database to authenticate server certificates. This database may be used in addition to the WellKnownTrustedCAs.class and CustomizedCAs.p12 files.

If you are running on a Windows system and you are using certificates from CAs, which are not in the WellKnownTrustedCAs.class file that exists in the Microsoft cryptographic database, then you may wish to use this method for authenticating the server to avoid administrative overhead. If your CA is not listed in the cryptographic database or you are using a self-signed certificate, you may add it to that database. Follow the instructions that are provided by the browser.

12.3 Certificate management utility

The IBM certificate management utility, a Java application, is available on the following platforms:

- Microsoft Windows
- AIX
- OS/400

The zSeries administrators may use gskkyman or RACF to manage their certificates. Refer to 3.6, “Using SSL with Communications Server for z/OS” on page 90 for specific information for the zSeries platform.

Servers on platforms other than Windows, AIX, and zSeries have no Host On-Demand utility for adding unknown CAs to the HODServerKeyDb.kdb file. There is a Java utility that may be used to insert the server’s public key certificate into the CustomizedCAs.p12 file, `keyrng`. Refer to 12.5, “The P12 keyring utility” on page 498 for details on this utility.

The following sections demonstrate the usage of the certificate management utility for:

- Requesting a certificate from an unknown CA and making it available to the clients
- Creating a self-signed certificate and making it available to the clients.

12.3.1 Starting the certificate management utility

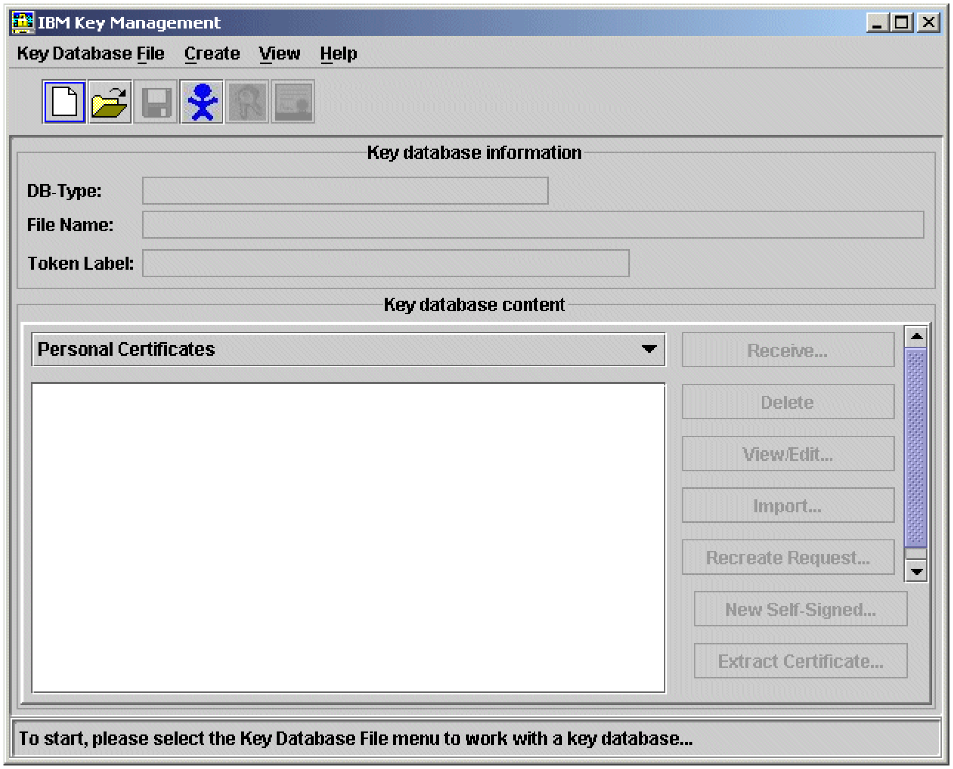
OS/390 or z/OS users should refer to 3.6.3, “SSL configuration using gskkyman” on page 93:

- To start the certificate management tool on OS/400, on the OS/400 command line, type `GO HOD`. Select option **5. Certificate Management** (WRKHODKYR).
- To start the certificate management utility on Windows click **Start** -> **Programs** -> **IBM Host On-Demand** -> **Administration** -> **Certificate Management**.
- Before running the certificate management utility on AIX, you must be in the `/HostOnDemand/bin` directory, and the JAVA_HOME environment variable must be set to the full path of your Java installation. For example, if the default installation options were chosen, you would run the certificate management utility by doing the following:

  ```
  cd /usr/opt/IBM/HostOnDemand/bin
  export JAVA_HOME=/usr/opt/HostOnDemand/jre/bin
  ./CertificateManagement
  ```

The graphical interface on Windows and AIX is the same.

The first window you will see is shown in Figure 12-1.



To start, please select the Key Database File menu to work with a key database...

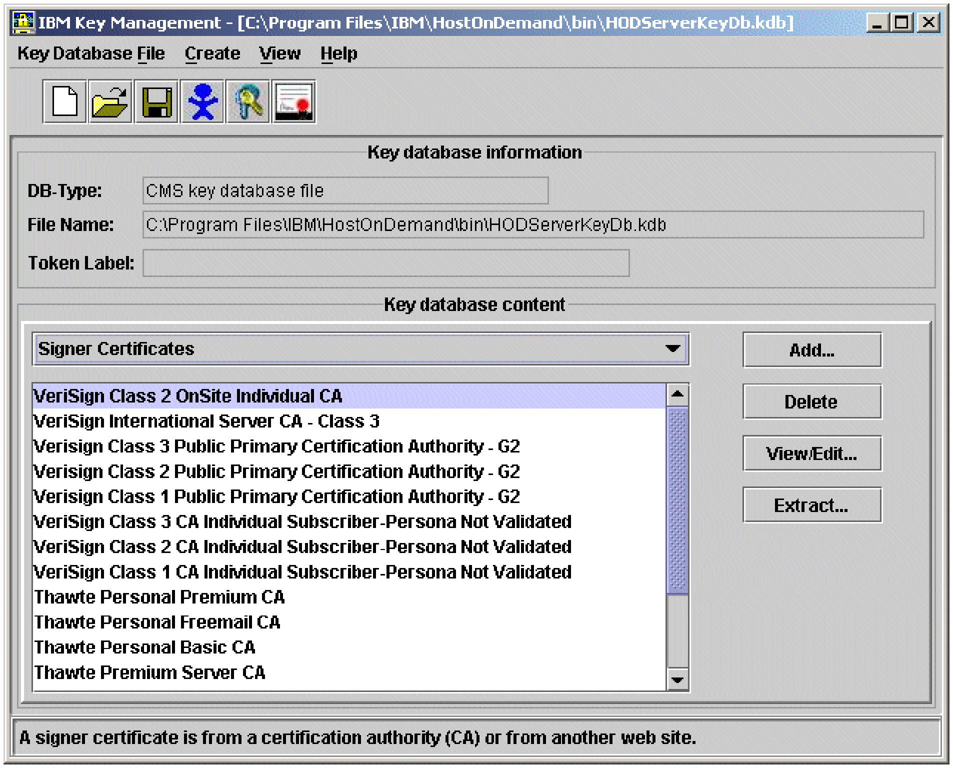
Figure 12-1 Certificate management utility

12.3.2 Create a request for an unknown CA

Here are the steps:

1. Click **KeyDatabaseFile** -> **New**.
2. Accept the CMS keyring database file, using `HODServerKeyDb.kdb` for the file name and `\HostOnDemand\bin` for the location. Click **OK**.
3. You may be asked if you want to replace an existing file. Click **Yes**.
4. The Password window appears. Enter your password twice and, if you wish, set an expiration time.
5. Select **Stash the Password to a file**. This will cause the password to be held, encrypted, in `\HostOnDemand\bin\HODServerKeyDb.sth`. The Host On-Demand server needs to be able to access it at runtime. Click **OK**.

6. Your Certificate Management window will look like Figure 12-2.



IBM Key Management - [C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb]

DB-Type: CMS key database file

File Name: C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb

Token Label:

VeriSign Class 2 OnSite Individual CA
VeriSign International Server CA - Class 3
Verisign Class 3 Public Primary Certification Authority - G2
Verisign Class 2 Public Primary Certification Authority - G2
Verisign Class 1 Public Primary Certification Authority - G2
VeriSign Class 3 CA Individual Subscriber-Persona Not Validated
VeriSign Class 2 CA Individual Subscriber-Persona Not Validated
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA

A signer certificate is from a certification authority (CA) or from another web site.

Figure 12-2 Create new certificate request - start

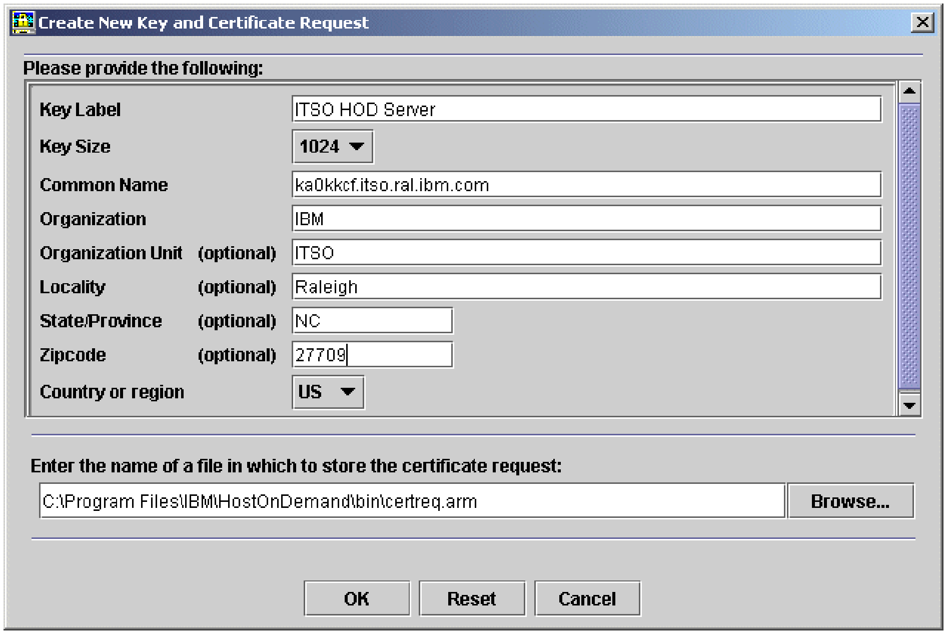
7. Select **Personal Certificate Requests** from the drop-down list.
8. Click **Create** and select **New Certificate request**. The Create New Certificate Request window appears.
9. Use Table 12-1 to enter your data in the appropriate fields, and enter a name and location for this file; in our example `\HostOnDemand\bin\certreq.arm`.

Table 12-1 Certificate request information

Field name	Value
Key Label	This field is for identification use only, so use a meaningful text string.
Version	Use X509 V3.
Key Size	This should default to the encryption level of your installation. The larger value is more secure, but you must take into account the capabilities of your browsers to decrypt.

Field name	Value
Common Name	This should be the fully qualified DNS name of the server. It will be used if any client requests server authentication, and when resolved by the DNS server it must match the IP address the client uses to establish the session.
Organization	Fully identify the name of your organization, for example IBM Corp.
Organizational Unit	This optional field can further identify the server or department operating the server within the organization, for example ITSO.
Locality	This optional field should contain the city where the server is located.
State/Province	This is an optional parameter.
Zipcode	This is an optional parameter. Some Netscape browser versions have been known to crash when this field is used; therefore, it is recommended that you omit this field.
Country	This will default to the native country code.

When complete, the window should look like Figure 12-3.



Please provide the following:

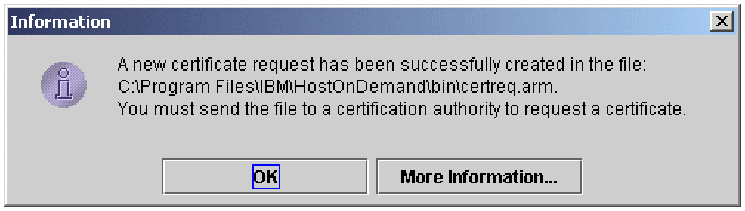
Key Label		ITSO HOD Server
Key Size		1024
Common Name		ka0kkcf.itso.ral.ibm.com
Organization		IBM
Organization Unit	(optional)	ITSO
Locality	(optional)	Raleigh
State/Province	(optional)	NC
Zipcode	(optional)	27709
Country or region		US

Enter the name of a file in which to store the certificate request:

C:\Program Files\IBM\HostOnDemand\bin\certreq.arm

Figure 12-3 Create new certificate request

10. Click **OK**. You will see a window similar to the one shown in Figure 12-4.



A new certificate request has been successfully created in the file:
C:\Program Files\IBM\HostOnDemand\bin\certreq.arm.
You must send the file to a certification authority to request a certificate.

Figure 12-4 Create new certificate request - completed

11. Note the file name and click **OK**.
12. Your certificate will appear in the list of Personal Certificate Requests.
13. Start a Web browser and access the CA's Web page. Follow the instructions provided to submit the certificate request. The following list provides the URLs of CAs:

    – VeriSign

      `http://www.verisign.com`

    – Thawte

      `http://www.thawte.com`

    Depending on the CA you choose, you can either e-mail the certificate request just generated, or incorporate the certificate request into the form or file provided by the CA.

    While you are waiting for the CA to process your certificate request, you can enable SSL security for controlled testing purposes only by using a self-signed certificate as described in 12.3.5, "Create a self-signed certificate" on page 486.

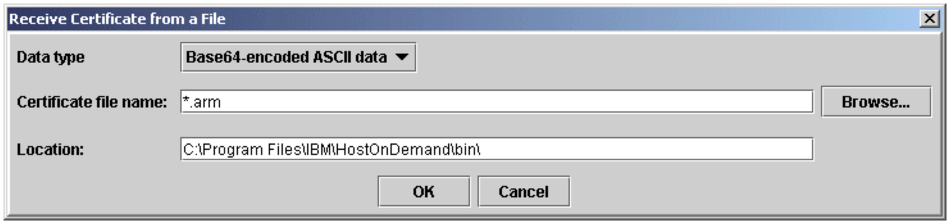
12.3.3 Receive the CA's certificate

When the certificate that was created in 12.3.2, "Create a request for an unknown CA" on page 479 has been signed and returned by the CA, you must receive it.

If your CA is already in your list of trusted CAs, you can skip directly to 12.3.4, "Receive the certificate signed by the CA" on page 484. To check this:

1. Click **KeyDatabaseFile** -> **Open** after you have started the certificate management utility as described in 12.3.1, "Starting the certificate management utility" on page 478.
2. Select the file, probably **HODServerKeyDb.kdb** in \HostOnDemand\bin, and click **Open**.

3. Select **Signer Certificates** from the drop-down list.
4. If there are no entries with the name of that CA, click **Add** and the window shown in Figure 12-5 will appear.



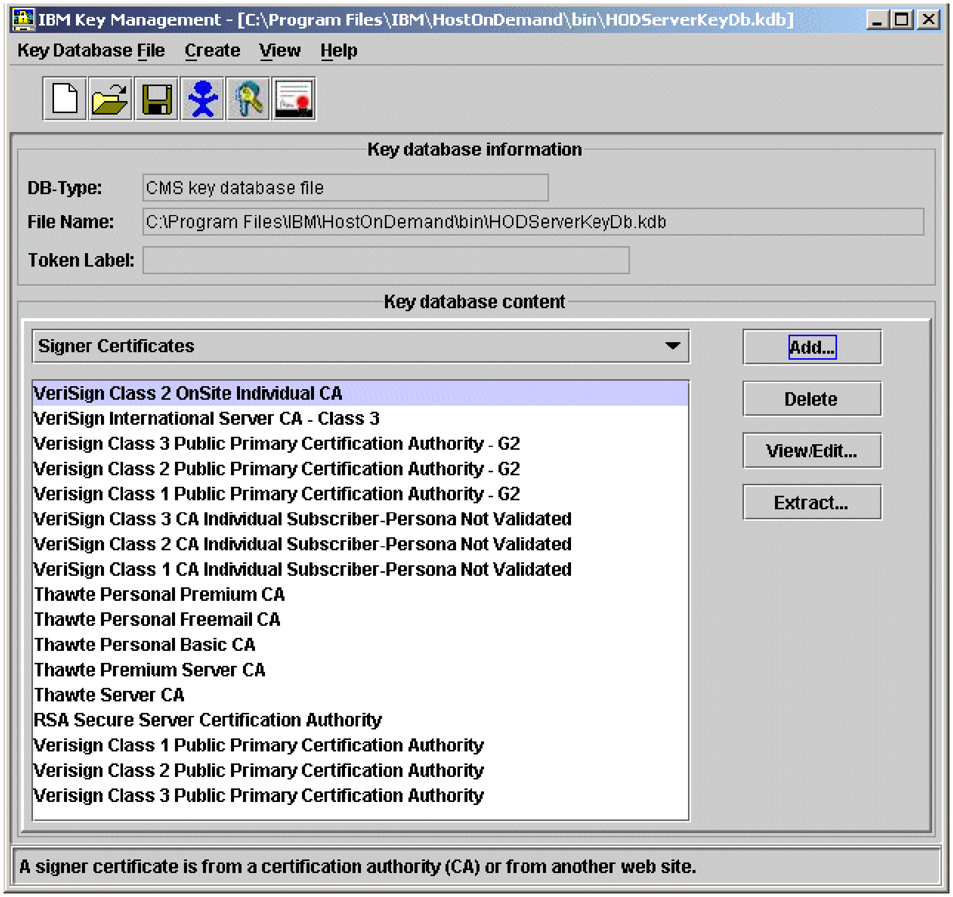
Data type: Base64-encoded ASCII data

Certificate file name: *.arm

Location: C:\Program Files\IBM\HostOnDemand\bin\

Figure 12-5 Receive CAs certificate

5. Enter the name of the file you have received and click **OK**.
6. Enter a meaningful label at the next window, for example TrustAuthorityCA and click **OK**.
7. The CA will be added to the list of Signer Certificates as shown in Figure 12-6.



IBM Key Management - [C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb]
Key Database File
Create
View
Help

Key database information

DB-Type: CMS key database file

File Name: C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb

Token Label:

Key database content

Signer Certificates

VeriSign Class 2 OnSite Individual CA
VeriSign International Server CA - Class 3
Verisign Class 3 Public Primary Certification Authority - G2
Verisign Class 2 Public Primary Certification Authority - G2
Verisign Class 1 Public Primary Certification Authority - G2
VeriSign Class 3 CA Individual Subscriber-Persona Not Validated
VeriSign Class 2 CA Individual Subscriber-Persona Not Validated
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority

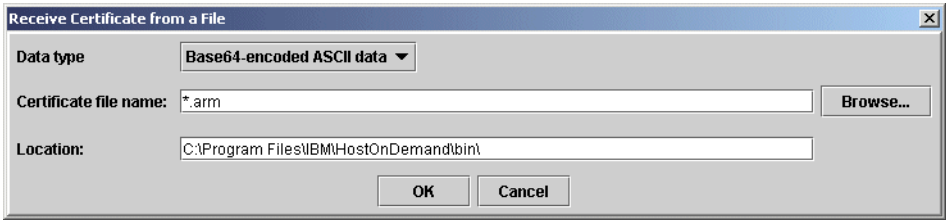
A signer certificate is from a certification authority (CA) or from another web site.

Figure 12-6 Receive CAs certificate - done

12.3.4 Receive the certificate signed by the CA

Here are the steps:

1. Assuming you have already opened the CMS keyring database file x:\HostOnDemand\bin\HODServerKeyDb.kdb, select **Personal Certificates** from the drop-down list.
2. Click **Receive** and the window shown in Figure 12-7 will appear.


Receive Certificate from a File

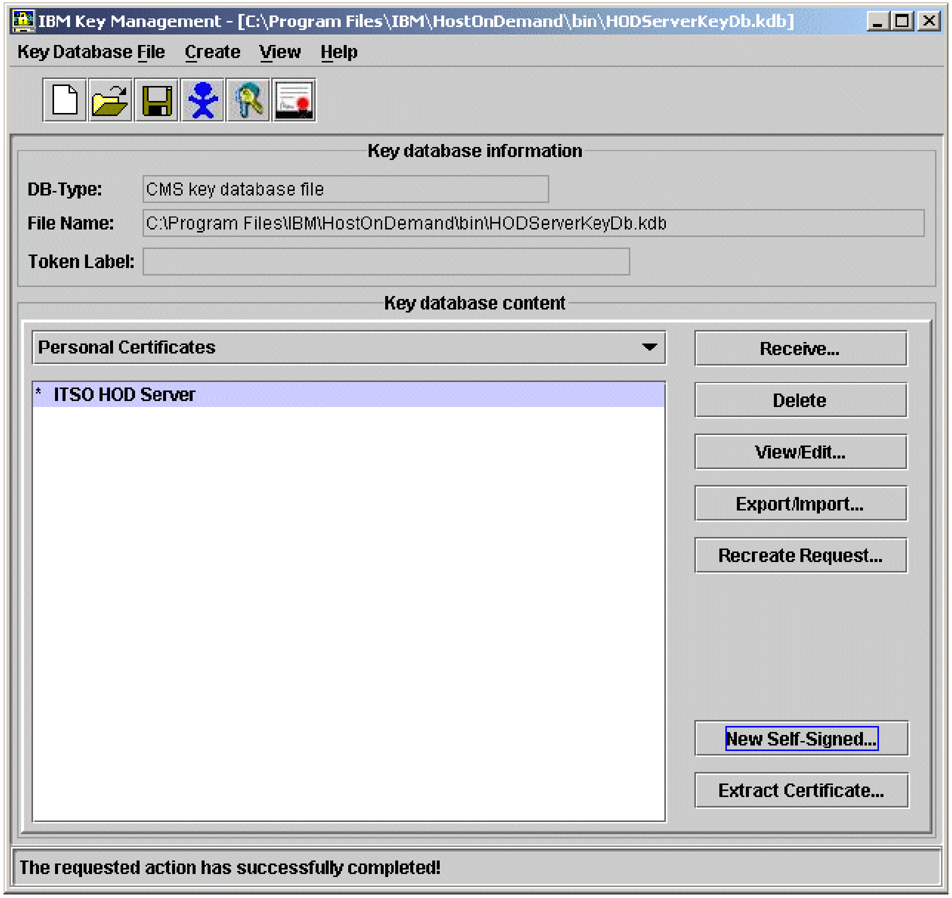
Data type: Base64-encoded ASCII data

Certificate file name: *.arm

Location: C:\Program Files\IBM\HostOnDemand\bin\

Figure 12-7   Receive signed certificate

3. Enter the name of the file you have received and click **OK**.
4. The CA will be added to the list of Personal Certificates as shown in Figure 12-8.


IBM Key Management - [C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb]

Key database information

DB-Type: CMS key database file

File Name: C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb

Token Label:

Key database content

Personal Certificates

* ITSO HOD Server

The requested action has successfully completed!

Figure 12-8   Receive signed certificate - done

5. In order for the Host On-Demand service manager to use this new certificate, you must stop and restart the Host On-Demand service manager.
6. Continue with 12.3.6, “Make a certificate available for the clients” on page 489.

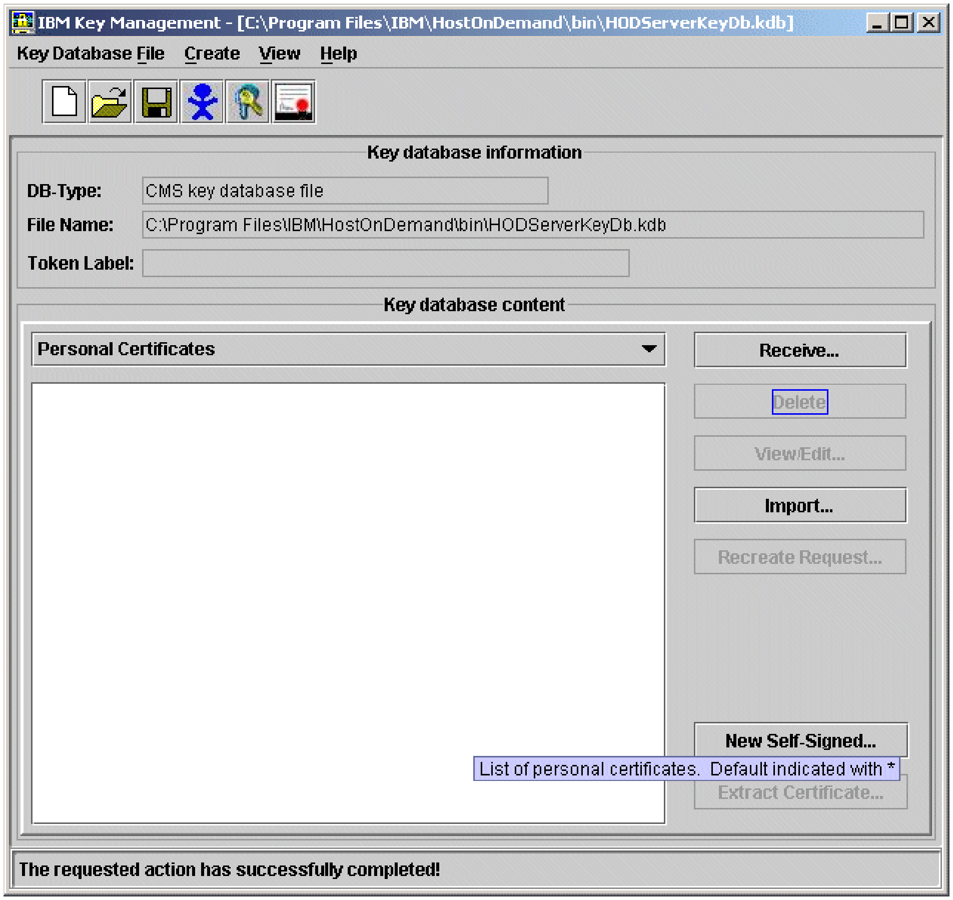
12.3.5 Create a self-signed certificate

Here are the steps:

1. After you have started the utility, click **KeyDatabaseFile** -> **New**.

> **Important:** If you want to use a self-signed certificate while you are waiting for a signed certificate to be returned from a CA, click **KeyDatabaseFile** -> **Open** instead, do *not* create a new database file. Skip to step 6.

2. Accept Key database type CMS, HODServerKeyDb.kdb for the file name and `x:\HostOnDemand\bin` for the location. Click **OK**.
3. You may be asked if you want to replace an existing file. Click **Yes**.
4. The Password window appears. Enter your password twice and, if you wish, set an expiration time.
5. Select **Stash the Password to a file**. This will cause the password to be held, encrypted, in \HostOnDemand\bin\HODServerKeyDb.sth. The Host On-Demand server needs to be able to access it at runtime. Click **OK**.
6. Select **Personal Certificates** from the drop-down list.
7. Your Certificate Management window will look like Figure 12-9.



DB-Type: CMS key database file

File Name: C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb

Token Label:

The requested action has successfully completed!

Figure 12-9 Create new self-signed certificate - start

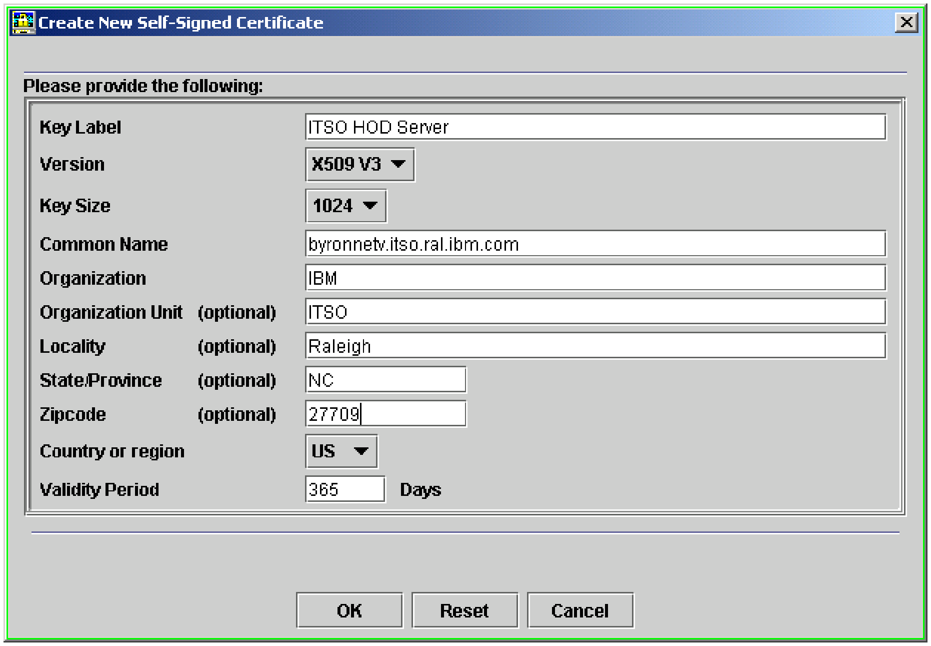
8. Click **New Self-signed Certificate**. The Create New Self-Signed Certificate window appears.
9. Use Table 12-2 to enter your data in the appropriate fields.

Table 12-2 Self-signed certificate information

Field name	Value
Key Label	This field is for identification use only, so use a meaningful text string.
Version	Use X509 V3.
Key Size	This should default to the encryption level of your installation. The larger value is more secure, but you must take into account the capabilities of your browsers to decrypt.

Field name	Value
Common Name	This should be the fully qualified DNS name of the server. It will be used if any client requests server authentication, and when resolved by the DNS server it must match the IP address the client uses to establish the session.
Organization	Fully identify the name of your organization, for example IBM Corp.
Organizational Unit	This optional field can further identify the server or department operating the server within the organization, for example ITSO.
Locality	This optional field should contain the city where the server is located.
State/Province	This is an optional parameter.
Zipcode	This is an optional parameter. Some Netscape browser versions have been known to crash when this field is used; therefore, it is recommended that you omit this field.
Country	This will default to the native country code.
Validity	The maximum recommended value is 365 days.

10. When complete, the window should look like Figure 12-10.


Create New Self-Signed Certificate

Please provide the following:

Key Label	ITSO HOD Server
Version	X509 V3
Key Size	1024
Common Name	byronnetv.itso.ral.ibm.com
Organization	IBM
Organization Unit (optional)	ITSO
Locality (optional)	Raleigh
State/Province (optional)	NC
Zipcode (optional)	27709
Country or region	US
Validity Period	365 Days

Figure 12-10 Create new self-signed certificate - completed

11.Click **OK**. Your certificate will appear in the list of Personal Certificates.

12.Use View/Edit to check that the values are correct and that the certificate is the default.

13.In order for the Host On-Demand service manager to use this new certificate, you must stop and restart the Host On-Demand service manager.

14.Continue with Make a certificate available for the clients.

12.3.6 Make a certificate available for the clients

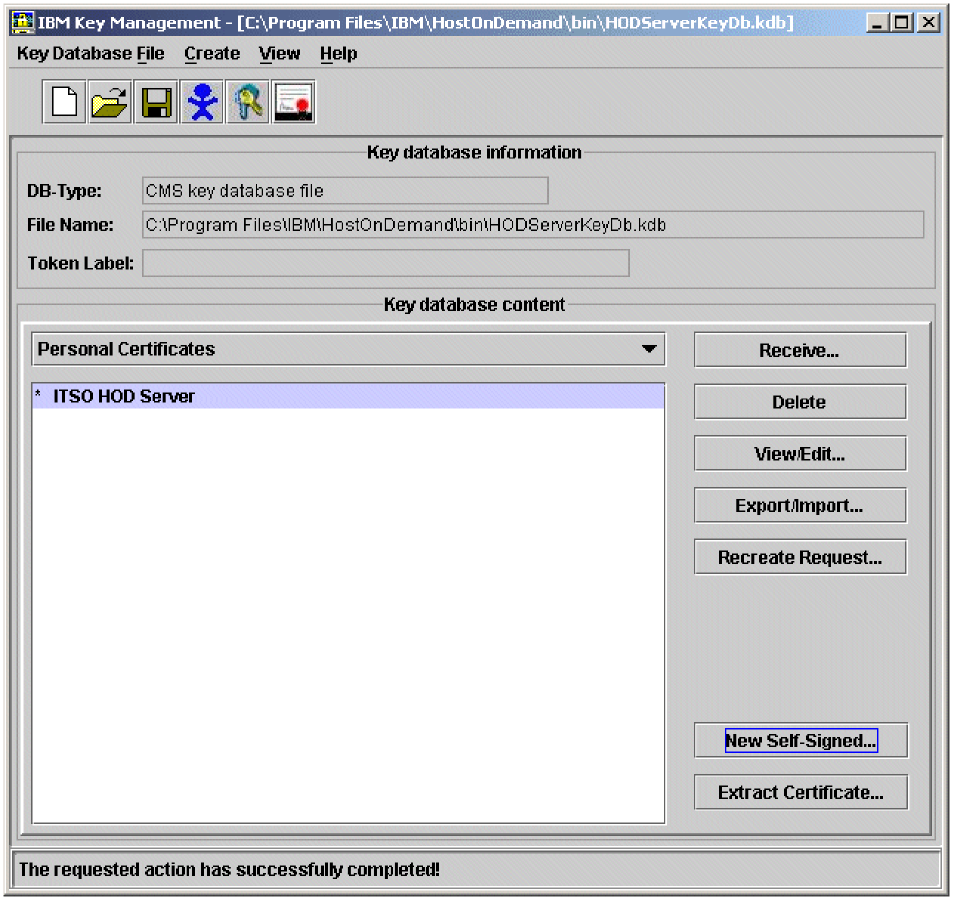
Here are the steps:

1. Start the Certificate Management utility on the Host On-Demand server and open the keyring database file, HODServerKeyDb.kdb, which is located in the \HostOnDemand\bin directory.

2. For a certificate from an unknown CA, select **Signer Certificates** from the drop-down list.

   For a self-signed certificate, select **Personal Certificates** from the drop-down list.

   Your window will look like Figure 12-11.


IBM Key Management - [C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb]

DB-Type: CMS key database file

File Name: C:\Program Files\IBM\HostOnDemand\bin\HODServerKeyDb.kdb

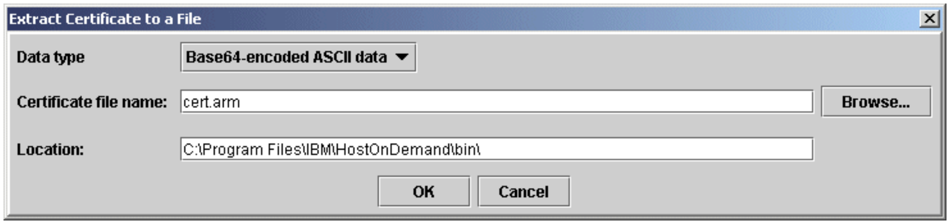
Token Label:

* ITSO HOD Server

The requested action has successfully completed!

Figure 12-11 Distribute self-signed certificate - selection

3. Highlight the certificate you want to make available for the clients.
4. Click **Extract Certificate** and the Extract Certificate to a File window appears.


Extract Certificate to a File

Data type: Base64-encoded ASCII data

Certificate file name: cert.arm

Location: C:\Program Files\IBM\HostOnDemand\bin\

Figure 12-12 Extract certificate

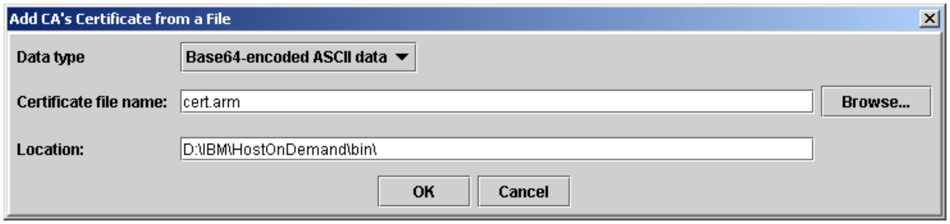
5. Change the `Data type` and the `Certificate file name` if required.

6. Click **OK** and the file will be created.
7. Close the keyring database file.
8. Click **KeyDatabaseFile** -> **New**.
9. Select **PKCS12** from the Key database type drop-down list, accept `CustomizedCAs.p12` for the file name and `\HostOnDemand\HOD\` for the location. Click **OK**.
10. You may be asked if you want to replace an existing file. In that case, click **Yes**.
11. The Password window appears. Enter `hod` as your password twice and, if you wish, set an expiration time.

> **Important:** At runtime, the client will access the CustomizedCAs.p12 file using the password **`hod`** as a hardcoded value. So, even if the utility allows you to enter any password, make sure you use `hod`.

12. Select **Stash the Password to a file**. This will cause the password to be held, encrypted, in \HostOnDemand\bin\HODServerKeyDb.sth. The Host On-Demand server needs to be able to access it at runtime. Click **OK**.
13. For a certificate from an unknown CA, select **Signer Certificates** from the drop-down list and click **Add**.

    For a self-signed certificate, select **Signer Certificates** from the drop-down list and click **Add**.
14. Select the Base64-encoded ASCII data from the Data type pull-down.
15. Enter the file name and location where you stored it, in our example `\HostOnDemand\HOD\bin\cert.arm`, or click **Browse** to locate it.



Add CA's Certificate from a File

Data type: Base64-encoded ASCII data

Certificate file name: cert.arm

Location: D:\IBM\HostOnDemand\bin\

Figure 12-13 Adding a Self-signed certificate

16. Click **OK** to insert the certificate.
17. Enter a meaningful label, for example TrustAuthorityCA and click **OK**.
18. The certificate will be added to the selected list.

19. Save and close the CustomizedCAs.p12 file.

You may also create and update the CustomizedCAs.p12 file using the Windows locally installed Host On-Demand client, and copy the file to the published directory of the server.

12.3.7 CustomizedCAs.p12 file background information

When Host On-Demand Version 8 is installed, the installation process migrates a existing CustomizedCAs.class file to the new format as CustomizedCAs.p12, leaving the old file in place. To start the migration tool manually on a Windows server, the appropriate commands are:

```
cd C:\Program Files\IBM\HostOnDemand\HOD

"C:\Program Files\IBM\HostOnDemand\jre\bin\java" -cp ..\lib\sm.zip
com.ibm.eNetwork.HOD.convert.CVT2PKCS12
<your_publish_directory>\Customized.CAs.class hod
```

(The command shown above should all be on one line.)

Note: If the migration tools detects both files, CustomizedCAs.class and CustomizedCAs.p12, no migration will be done.

The HOD V8 client is able to use both database formats (CustomizedCAs.p12 and CustomizedCAs.class). When a SSL-session is started, the client first checks for a CustomizedCAs.class file and than for a CustomizedCAs.p12 file. If neither of them is found the session will fail. Previous clients are only able to use a CustomizedCA.class file. So for backward compatibility *and* if both files exist already, the Certificate Management, when closed, will automatically keep the CustomizedCAs.class file up to date with the same certificates as in the CustomizedCAs.p12 file. This process, called *reverse migration* needs to be started manually on AIX servers.

To start the reverse migration manually on a Windows server, the appropriate commands are:

```
cd C:\Program Files\IBM\HostOnDemand\HOD

"C:\Program Files\IBM\HostOnDemand\jre\bin\java" -cp ..\lib\sm.zip
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT CustomizedCAs.p12 hod
Customized.CAs.class
```

(The command shown above should all be on one line.)

For further information, please refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301.

12.4 The IKEYCMD command-line tool

IKEYCMD is a command-line tool, in addition to the Host On-Demand Certificate Management utility, that can be used to manage keys, certificates, and certificate requests. It is functionally similar to Certificate Management and is meant to be run from the command line without a graphical interface. It can be called from native shell scripts and programs to be used when applications prefer to add custom interfaces to certificate and key management tasks. It can create key database files for all of the types that the Certificate Management utility currently supports. It can create certificate requests, import CA-signed certificates, and manage self-signed certificates. It is Java-based, and is available only on Windows and AIX platforms.

Use IKEYCMD for configuration tasks related to public-private key creation and management. You cannot use IKEYCMD for configuration options that update the server configuration file, httpd.conf. For options that update the server configuration file, you must use the IBM Administration Server.

12.4.1 Environment set-up for IKEYCMD command-line interface

Set up the environment variables to use the IKEYCMD command-line interface as follows:

- For Windows platforms, do the following:
  - Using the user interface or by modifying autoexec.bat on a command window, set/modify the PATH variable to include the location of the Java executable files:

    ```
    set PATH=c:\Program Files\IBM\HostOnDemand\bin;%PATH%;
    ```

  - Using the user interface or by modifying autoexec.bat on a command window, set/modify the CLASSPATH environment variable as follows:

    ```
    set CLASSPATH=c:\Program Files\IBM\GSK6\classes\cfwk.zip;C:\
    Program Files\IBM\GSK6\classes\gsk6cls.jar;%CLASSPATH%;
    ```

- For AIX platforms:
  - First ensure that your xlC files (which constitute the run-time library for the standard AIX C++ compiler) meet one of the following requirements:
    - On AIX 4.3: fileset xlC.aix43.rte must be at level 5.0.2.0 or later
    - On AIX 5.2: fileset xlC.aix50.rte must be at level 6.0.0.3 or later

    Use the following command to confirm your version:

    ```
    lslpp -ha "xlC.aix*.rte"
    ```

    (If your xlC fileset is outdated and you start the Host On-Demand ServiceManager with Certificate Management active, errors occur.)

- Next make the following specifications:
  - Set your PATH to where your Java or JRE executable resides:

    ```
    EXPORT PATH=/opt/IBM/HostOnDemand/jre:$PATH
    ```

  - Set the following CLASSPATH environment variable:

    ```
    EXPORT CLASSPATH=/usr/opt/ibm/gskak/classes/cfwk.zip:/
    usr/opt/ibm/gskak/classes/gsk6cls.jar:$CLASSPATH
    ```

  Once you have completed these steps, IKEYCMD should run from any directory.

To run an IKEYCMD command, use the following syntax:

```
java com.ibm.gsk.ikeyman.ikeycmd <command>
```

12.4.2 IKEYCMD command-line syntax

The syntax of the Java CLI is:

```
java [-Dikeycmd.properties=<properties_file>],
com.ibm.gsk.ikeyman.ikeycmd <object> <action> [options]
```

Where

- -Dikeycmd.properties specifies the name of an optional properties file to use for this Java invocation. A default properties file, ikminit_hod.properties, is provided as a sample file that contains the default settings for Host On-Demand:
  - For Windows platforms, a sample properties file, ikm0init_hod.properties, is supplied in your_install_directory\bin, where your_install_directory is your Host On-Demand installation directory.
  - For AIX platforms, this file is supplied in your_install_directory/bin.

- The following table describes each action that can be performed on a specified object.

Table 12-3 IKEYCMD command line parameter overview

Object	Action	Description
-keydb	-changepw	Change the password for a key database
	-convert	Convert the key database from one format to another
	-create	Create a key database
	-delete	Delete the key database
	-stashpw	Stash the password of a key database into a file
-cert	-add	Add a CA certificate from a file into a key database
	-create	Create a self-signed certificate
	-delete	Delete a CA certificate
	-details	List the detailed information for a specific certificate
	-export	Export a personal certificate and its associated private key from a key database into a PKCS#12 file, or to another key database
	-extract	Extract a certificate from a key database
	-getdefault	Get the default personal certificate
	-import	Import a certificate from a key database or PKCS#12 file
	-list	List all certificates
	-modify	Modify a certificate (NOTE: Currently, the only field that can be modified is the Certificate Trust field)
	-receive	Receive a certificate from a file into a key database
	-setdefault	Set the default personal certificate
	-sign	Sign a certificate stored in a file with a certificate stored in a key database and store the resulting signed certificate in a file

Object	Action	Description
-certreg	-create	Create a certificate request
	-delete	Delete a certificate request from a certificate request database
	-details	List the detailed information of a specific certificate request
	-extract	Extract a certificate request from a certificate request database into a file
	-list	List all certificate requests in the certificate request database
	-recreate	Recreate a certificate request
-help		Display help information for the IKEYCMD command
-version		Display IKEYCMD version information

Table 12-4 IKEYCMD command-line options overview

Option	Description
-db	Fully qualified path name of a key database
-default_cert	Sets a certificate to be used as the default certificate for client authentication (yes or no). The default is no.
-dn	X.500 distinguished name. Input as a quoted string of the following format (only CN, O, and C are required): "CN=Jane Doe,O=IBM,OU=Java Development,L=Endicott, ST=NY,ZIP=13760,C=country"
-encryption	Strength of encryption used in certificate export command (strong or weak). The default is strong.
-expire	Expiration time of either a certificate or a database password (in days). Defaults are 365 days for a certificate and 60 days for a database password.

Option	Description
-file	File name of a certificate or certificate request (depending on specified object)
-format	Format of a certificate (either ascii for Base64_encoded ASCII or binary for Binary DER data). The default is ascii.
-label	Label attached to a certificate or certificate request
-new_format	New format of key database
-new_pw	New database password
-old_format	Old format of key database
-pw	Password for the key database or PKCS#12 file. See Creating a new key database.
-size	Key size (512 or 1024). The default is 1024.
-stash	Indicator to stash the key database password to a file. If specified, the password will be stashed in a file.
-target	Destination file or database.
-target_pw	Password for the key database if -target specifies a key database. See Creating a new key database.
-target_type	Type of database specified by -target operand (see -type).
-trust	Trust status of a CA certificate (enable or disable). The default is enable.
-type	-type Type of database. Allowable values are cms (indicates a CMS key database), webdb (indicates a keyring), sslight (indicates an sslight .class), or pkcs12 (indicates a PKCS#12 file).
-x509version	Version of X.509 certificate to create (1, 2 or 3). The default is 3.

12.4.3 Example: Creating a self-signed certificate

It usually takes two to three weeks to receive a certificate from a well-known CA. While waiting for an issued certificate, use IKEYCMD to create a self-signed server certificate to enable SSL sessions between clients and the server. Use this procedure if you are acting as your own CA for a private Web network.

For Windows platforms for example, to create a self-signed certificate, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -size <1024 | 512> -dn <distinguished name>
-label <label> -default_cert <yes or no>
```

where your_install_directory is your Host On-Demand installation directory. Note the following descriptions:

-size: Key size 512 or 1024

-label: Enter a descriptive comment used to identify the key and certificate in the database.

-dn: Enter an X.500 distinguished name. This is input as a quoted string of the following format (Only CN, O, and C are required; CN=common_name, O=organization, OU=organization_unit,L=location, ST=state, province, C=country).

"CN=weblinux.raleigh.ibm.com,O=ibm,OU=IBM HTTP Server,L=RTP,ST=NC,C=US"

-default_cert: Enter `yes`, if you want this certificate to be the default certificate in the key database. If not, enter No.

For more in-depth information, see *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301 which comes with the product.

12.5 The P12 keyring utility

The keyring utility is used to obtain a site or server certificate from a Telnet server (or Redirector) and install it into the CustomizedCAs.p12 file. It is provided for servers that do not have the certificate management utility. The Java keyring utility is shipped with Host On-Demand and uses lengthy commands, so it is easy to make errors. On iSeries and Windows systems a script file is shipped; however, you can create your own script file. The example below was created for the zSeries server that was discussed in “Make certificates available to clients” on page 103. We created a shell script **javakeyrng** with the command so it could be reissued if needed. The backslash is a continuation character; otherwise, the command must be on one continuous line. The command for Java 1.4 is:

```
java -classpath .;/usr/lpp/HOD/hostondemand/lib/sm.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs connect ipaddr:port
```

Where `ipaddr` is the address of your TN3270 Telnet server, and `port` is the SSL port you wish to connect. If no port is provided, the well-known secure Telnet or FTP port is used.

> **Tip:** If you would like to set up a SSL connection using the Redirector, use the port number of the secure port that you have defined in the redirector to be used by your secure sessions (for example 12173).

The command for Java 1.1.8 is:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:$CLASSPATH \
com.ibm.hodsslight.tools.keyrng CustomizedCAs \
connect ipaddr:port
```

You will be prompted to enter the password for CustomizedCAs.p12 file. AT runtime, the clients will access the file using the password hod, so enter `hod` as the password and press Enter. The results of the command will look similar to the Java 1.4 example shown in Example 12-1.

Example 12-1   Java keyring utility output

```
CASEY @ SC48:/usr/lpp/HOD/hostondemand/HOD>javakeyrng
Password for CustomizedCAs.class:
Connecting to 9.12.6.126:6623
com.ibm.hodsslight.SSLException
        at com.ibm.hodsslight.SSLConnection.certificate(SSLConnection.java:979)
        at com.ibm.hodsslight.SSLClient.serverCertificate(SSLClient.java:272)
        at com.ibm.hodsslight.SSLClient.handshake(SSLClient.java:110)
        at
com.ibm.hodsslight.SSLConnection.handleData(SSLConnection.java(Compiled Code))
        at
com.ibm.hodsslight.SSLRecordLayer.receiveRecord(SSLRecordLayer.java:695)
        at com.ibm.hodsslight.SSLConnection.install(SSLConnection.java:212)
        at com.ibm.hodsslight.SSLClient.<init>(SSLClient.java:719)
        at com.ibm.hodsslight.SSLSocket.install(SSLSocket.java:117)
        at com.ibm.hodsslight.SSLSocket.<init>(SSLSocket.java:260)
        at com.ibm.hodsslight.tools.keyrng.main(keyrng.java)
com.ibm.hodsslight.SSLException
 time created=Wed Aug 29 16:52:27 EDT 2001
 category=4  TRUSTPOLICY
 error=1017  PEERCERTIFICATECHAINNOTTRUSTED
 int1 =0
 e=null

-------------------------- Server Certificate Chain --------------------------

Site Certificate - Number 0

        Key : RSA/512 bits
     Subject: wtsc48oe.itso.ibm.com, Research Triangle Park, ITSO, IBM, US
      Issuer: ITSORaleigh, Raleigh, ITSO, IBM, US
  Valid from: Mon Aug 27 10:53:17 EDT 2001
    Valid to: Tue Aug 27 11:03:17 EDT 2002
Finger print: 2A:84:BA:46:C0:73:7C:4F:6D:98:AD:B1:44:72:BA:F8

------------------------------------------------------------------------------

Enter the number of the certificate to be added to CustomizedCAs.p12 (q to
quit): 0
Adding the Site Certificate - 0 to CustomizedCAs.p12
Done.
```

When executing in a Java 1.4 environment, we found that the flow of execution changes, since Java 1.4 classifies certain exception conditions different from Java 1.1.8. The result is that program flow under Java 1.4 follows a different exception handling path, a path not traversed under Java 1.1.8. In any case, the Java exception shown in Example 12-1 can be ignored. You can verify the certificate was added to the CustomizedCAs.p12 file using the following command:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs verify
```

The add option does not require the TN3270 server to be available, since no socket call is issued. You have to specify the name of the certificate file as one of the input parameters. The command when using Java 1.4 is:

```
java -classpath .;/usr/lpp/HOD/hostondemand/lib/sm.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs \
add --certificatetype certificate.name
```

where --`certificate type` is either `ca` if you are adding a CA root certificate, or `site` if you are adding a site or self-signed certificate. The `certificate.name` is the fully qualified name of the actual certificate, for instance, `/u/casey/itso.cer`.

The command for Java 1.1.8 is:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:$CLASSPATH \
com.ibm.hodsslight.tools.keyrng CustomizedCAs \
add --certificatetype certificate.name
```

13

Deployment strategies

IBM WebSphere Host On-Demand can provide cost effective and secure browser-based host access to users in both intranet and extranet-based environments. Host On-Demand is installed on a Web server, simplifying administrative management and deployment. The Host On-Demand applet is downloaded to the client's browser providing user connectivity to critical host applications and data.

This chapter discusses issues involved with deploying Host On-Demand. Careful consideration of these topics is important for successful deployment:

- Configuration models
- Client type - cached or download
- Client preload and Java considerations
- Security requirements
- Base platform(s) for Host On-Demand server

We advocate making these decisions with the goal of minimizing Host On-Demand administration and support requirements. This chapter will examine the factors that affect these choices, and why a particular choice should be made.

13.1 Host On-Demand configuration models

Default HTML files are shipped with Host On-Demand. Before clients can connect to sessions through the default pages, the administrator must log on to the Administration utility and configure user ID and session information. Some of the features available through the Deployment Wizard are not available with the default HTML pages. For example, using the Deployment Wizard, the administrator can select the level of client Java or tailor the preload components to be downloaded to clients. As it is recommended to use the Deployment Wizard, we will now review the configuration models available.

The Deployment Wizard requires the administrator to choose one of three configuration models. Choosing how the Host On-Demand server will communicate configuration information to the Host On-Demand client involves understanding the three types of configuration models available:

- Configuration server-based model
- Combined model
- HTML-based model

It may be that using only one model will not work for all your Host On-Demand users. Using the Deployment Wizard, Chapter 14, "Deployment Wizard" on page 517, the administrator can easily select the configuration model to be deployed to the Host On-Demand client.

When deciding which one of the three configuration options to use, you should consider the following:

- Do your users expect their individual preferences to be migrated with them from workstation to workstation?
- As the Host On-Demand administrator, how do you expect to access, manage, and change Host On-Demand user IDs and groups?
- Can you configure all the firewalls in your network to allow the passing of Host On-Demand configuration information between the workstation and Host On-Demand configuration server?
- Will there be performance issues on the Host On-Demand server caused by the number of users you have defined logging into the Host On-Demand server, and accessing their personalized configurations?
- Do you require one of the following services that require the Host On-Demand Service Manager, Redirector, License Use Management, or OS400 Proxy support?

13.1.1 HTML-based model

In the HTML-based model, session information is contained in HTML files created by the Deployment Wizard. Changes made by the end user, such as changing a screen color or keyboard mapping (if allowed), are stored locally on the user's machine. The Host On-Demand Service Manager/configuration server is not used to store or manage configuration data. After the end user has accessed the customized HTML page for the first time, information is then stored locally on the client's workstation. As a consequence, if the Host On-Demand server becomes unavailable but the Web server is available, the end user will be able to connect to their host sessions. This model does not require a firewall port to be opened to access the configuration server.

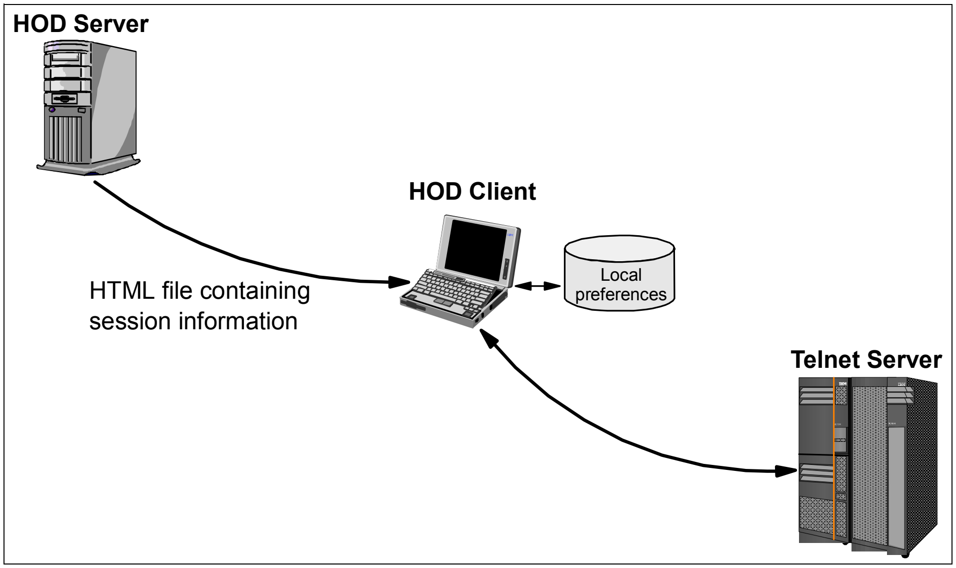


Figure 13-1 HTML-based model

Note: If License User Management is enabled, the client will attempt to communicate with the Host On-Demand Service manager. If there is an intervening firewall, it will need to be configured to allow access to the Host On-Demand Service Manager (port 8999 by default).

With the HTML-based model, the administrator sets up the initial session configuration windows and may choose to lock certain properties to prevent users from changing these fields. The administrator can also allow users to make session changes but not allow changes to be saved beyond the current session.

If the end user sets up personalized changes and the administrator later updates the customized HTML file through the Deployment Wizard, these updates will be merged with the updates made by the end user. However, if an end user has changed a field, changes stored in the end user's local file will override the updates made by the administrator. The administrator may override a user setting by setting the field value and locking the field.

Advantages:

- Access to the configuration server is not required (unless the Host On-Demand services, such as the Redirector, OS/400 proxy, or license use management, are enabled). Improved performance on the server may be realized, since these users are not accessing personalized configuration data.
- There is no need to open a separate port on the firewall as the configuration server is not accessed.
- There is no need to create and maintain Host On-Demand user IDs.
- End users are not required to logon to Host On-Demand.
- Performance may be better than using the configuration server because you do not have large numbers of users accessing personalized configurations on the configuration server.

Limitations:

- If users make changes to their personal configurations, those changes may not be available on other workstations without physically copying the files or placing them on a shared file system where they may be accessible from another workstation.

> **Note:** The HTML-based model is the default model used by the Deployment Wizard.

13.1.2 Configuration server-based model

In this model, session configuration data is stored and managed on the Host On-Demand configuration server by the administrator using the Host On-Demand Administration utility. End users must log on to the Host On-Demand configuration server with a user ID. A user ID may be shared among multiple end users. However, this is not recommended if the administrator is going to allow end users to save their user preferences. User IDs can also be grouped together if they share common configuration data. It may be easier to maintain configurations at a group level, especially if there is a large user base.

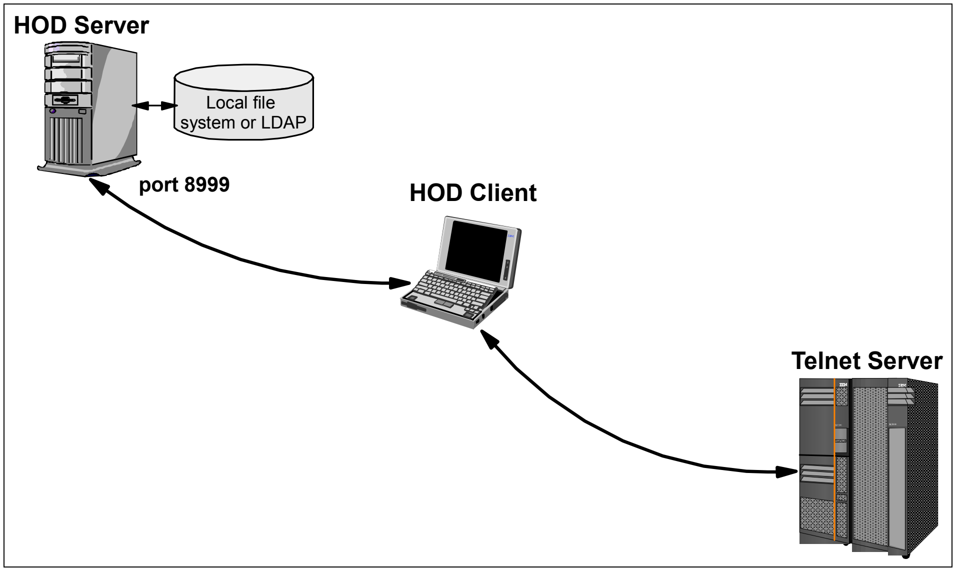


Figure 13-2 Configuration server-based model

If there is a firewall between the HOD server and the HOD client, the port used to communicate with the Host On-Demand configuration server (default is port 8999) must be opened in the firewall. If the Host On-Demand configuration servlet (refer to Chapter 9, “Configuration servlet” on page 387) is implemented, the port to the configuration server is not required.

Individual user preferences within a group are maintained with the user ID. This implies that if a user ID is a member of more than one group, each group may have group-specific session data but the user-specific data remains constant across the groups. This also means that if you have multiple HOD users logging onto HOD with the same user ID, allowing them to save preferences may cause conflicts as each user tries to save their own preferences. In this situation it is best to disallow users from saving preferences.

Advantages:

- Users can access their own personalized configuration data from any machine that has network access to the configuration server.
- Administrators can maintain the sessions from local or remote sites.
- Users may be able to be organized into groups, which simplifies administration.
- On the Windows, AIX and z/OS platforms, Native Authentication may be used to reduce the number of user IDs and passwords users are required to

remember. See 11.11, “Native Authentication” on page 453 for additional details.

Limitations:

- Administrative overhead of maintaining the configuration server user IDs, and groups.
- Performance implications if a large number of users are accessing the configuration server.
- Users must log on to Host On-Demand.
- Requires firewall port to configuration server to be opened, or use of the Host On-Demand config servlet.
- Must maintain and manager user IDs

Integrated Windows domain logon

For cases where the administrator chooses to have user settings stored on the Host On-Demand server, the user creation process can be automated if the clients are running on a Microsoft Windows operating system. If this option is selected, each user ID is identified to Host On-Demand by the user’s Windows Domain user name. Users are not prompted for a user name or password, but instead, the Windows domain security is relied upon for authentication. When this option is selected, the administrator specifies a default group for users that have not chosen to customize any settings. The first time a user customizes a setting, that user becomes defined on the Host On-Demand server, and the customizations are stored. For additional information on the integrated Windows domain logon, refer to 11.12, “Integrated Windows domain logon” on page 460.

13.1.3 Combined model

In the combined model, the administrator sets up a group on the configuration server with the required sessions (similar to the configuration server-based model). The Deployment Wizard is then used to create the HTML file specifying the group on the configuration server that will be accessed to obtain session information. Access to session information on the Host On-Demand configuration server is required the first time a client accesses a combined model HTML file. Like the configuration server-based model, if there is a firewall between the HOD server and the HOD client, the port used to communicate with the Host On-Demand configuration server (default is port 8999) must be opened in the firewall. If the Host On-Demand configuration servlet is implemented, the port to the configuration server is not required.

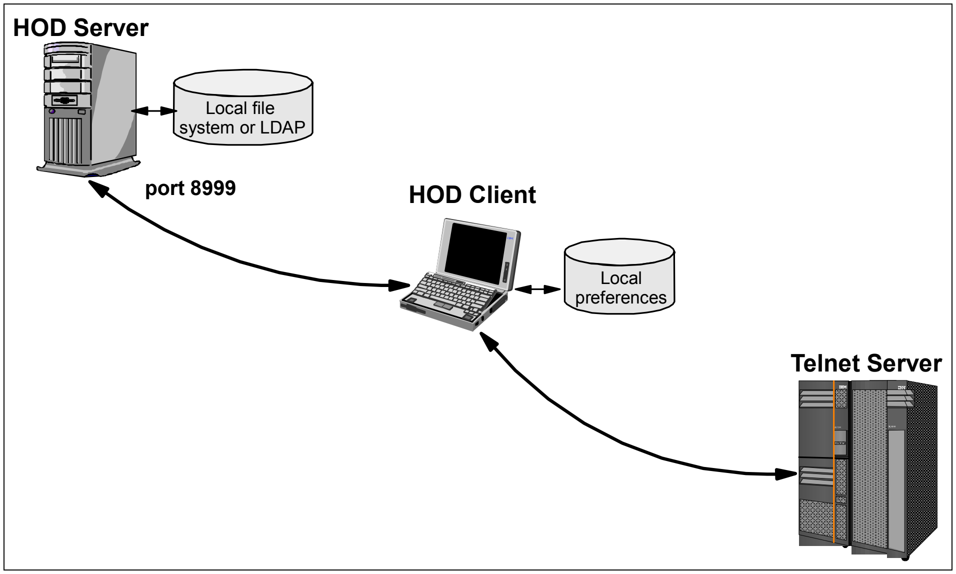
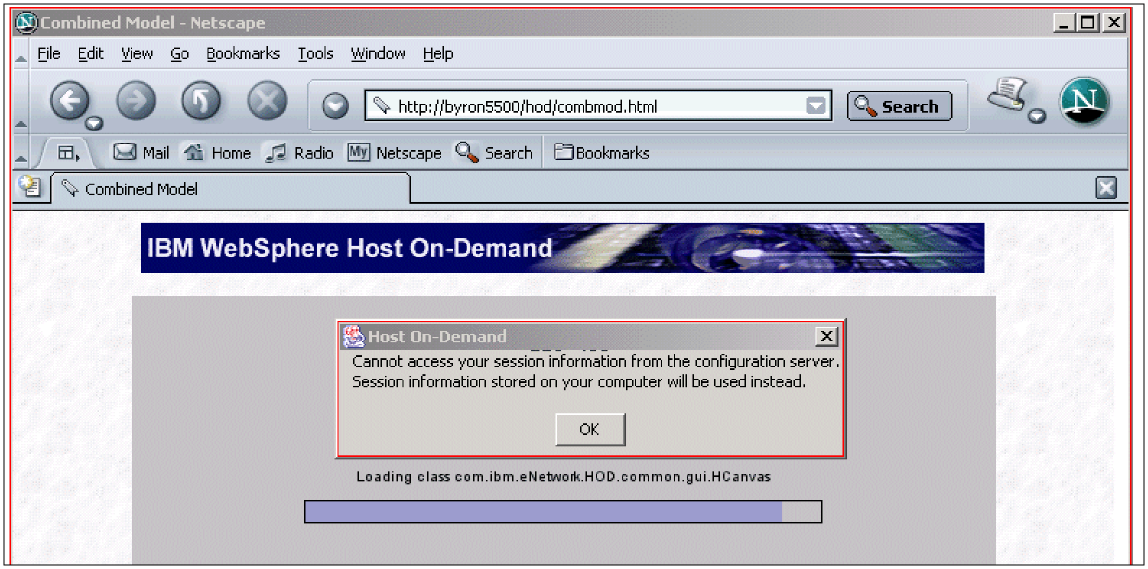


Figure 13-3 Combined model

After the initial access, if allowed by the administrator, user preferences are stored on the user's local machine (similar to the HTML model) and the Host On-Demand Service manager is not required, although if it is not running, users will see the screen as shown in Figure 13-4.


Combined Model - Netscape
File Edit View Go Bookmarks Tools Window Help
http://byron5500/hod/combmod.html
Search
Mail Home Radio Netscape Search Bookmarks
Combined Model
IBM WebSphere Host On-Demand
Host On-Demand
OK

Cannot access your session information from the configuration server.
Session information stored on your computer will be used instead.

Loading class com.ibm.eNetwork.HOD.common.gui.HCanvas

Figure 13-4 Combined model - no Service Manager

Advantages:

- At least one group must be created on the configuration server, but there is no requirement to create or maintain user IDs.
- Clients will attempt to access the configuration server before each use of Host On-Demand, but if the Configuration Server is unavailable, Host On-Demand clients will run using saved copies of the session configuration information.
- Administrators can update the group session information locally or remotely, and have it deployed to all clients the next time Host On-Demand is used. The updates are merged with the user's preferences. Any fields changed by the administrator will override the user preference. However, user-specified preferences are maintained for fields not changed by the administrator.
- On the Windows, AIX and z/OS platforms, Native Authentication may be used to reduce the number of user IDs and passwords users are required to remember. See 11.11, "Native Authentication" on page 453 for additional details.

Limitations:

- Configuration information on a local machine is not available to other machines unless it is physically copied or by placing them on a shared file system where they may be accessed by another workstation.
- This may increase administration overhead if there are a large number of "default" groups. Since there are no user IDs, the administrator must be aware of what "default" group a user is mapping to. Any changes to the group information will affect all users whose HTML files specify that group.
- This requires firewall port to configuration server to be opened or use of the Host On-Demand config servlet.

> **Note:** It is possible to for some users to access the configuration server and other users to implement the HTML-based or combined model. The administrator selects the model when using the Deployment Wizard.

13.1.4 User preferences

The administrator can restrict the settings that a user can change by locking the field. If the administrator does not lock a field but **Do not save preferences** is checked, changes made by the end user will not persist when they close the host session. The administrator can, after the initial deployment, change a default setting. Provided a user has not modified the setting, the new value will take effect the next time the user starts the Host On-Demand session. To override any settings that have been modified by the user, the administrator can set the value for the field and lock the field. The new value will take effect the next time the user starts the Host On-Demand session.

You may wish to consider the following when deciding to allow users to save preferences:

- Are individual user preferences required at all, or can you provide default settings that will meet the needs of your end users?
- Do you wish to have user preferences stored on the configuration server, or stored locally on end user's machines?
- Will users be moving between different workstations and require their user preferences to follow them?

Your answers to these questions should assist you in determining if you need to allow users to save preferences.

Some examples of customizations that may be required by end users are:

- Selecting a specific LU name or workstation ID
- Defining macros
- Personal color or keyboard settings

> **Hint:** Host On-Demand V8 provides the ability to code HTML overrides that allow a server side program to dynamically set various client side parameters. See Chapter 18, “Modifying session properties dynamically (using HTML overrides)” on page 631. This new functionality may reduce your need to permit individual user preferences since you can now programmatically change user settings based on such criteria as the IP address of the user.

13.2 Host On-Demand emulator clients

The HTML files created by the Deployment Wizard and loaded into the client browser launch the Host On-Demand emulator client. There are two different types of Host On-Demand emulator clients available:

- Download Client
- Cached Client

Some of the issues to consider before deciding which emulator client to use are:

- Level of Java installed in your client's browsers
- Network connection speeds

- Users access to multiple Host On-Demand servers using different levels of Host On-Demand code
- Type of Host On-Demand configuration model you wish to deploy

More detailed information on these clients can be found in Chapter 5, “Clients” on page 149. That chapter also discusses several issues of concern when deploying these Host On-Demand clients to your users.

Specifically, as the HOD administrator you should be aware of these issues and how they will affect users of HOD clients:

- 5.9, “Java 2 support” on page 179
- 5.10, “Java 2 practical issues” on page 185
- 5.11, “Client Java type: Java 1, Java 2, or Autodetect” on page 192
- 5.13, “Download client and cached-client implementation” on page 199
- 5.16, “Web browsers: Java 1 and Java 2 enabled” on page 213

13.3 Security requirements

One of the most fundamental considerations in building a secure Host On-Demand environment is to remember its Web-based nature. Restricting access to the Host On-Demand Web pages through Web server security is the first line of defense.

Having registered users, where they are required to log in to use the HOD service, is not primarily for security, but to aid in administration, and also for storing of the user’s preferences. Client authentication can be used to provide a high-security environment with standard PKI tools, and in concert with an established security management framework (for example, RACF).

The Telnet server is the next tine of defense. SSL can be used in order to prevent frame examination, and non-standard Telnet ports should be used to discourage discovery of the Telnet port you are using.

In its simplest form, Host On-Demand is simply a standard TN3270, TN5250 or VT client. While they may be suitable for intranet use, it is important to note that these standard terminal types (whether they are Host On-Demand or other software) cannot be considered secure. TN3270, for example, passes all data in the clear. A simple frame trace of TN3270 traffic on a network is enough to recover data, user ID information, and even mainframe passwords. Host On-Demand was the first Telnet emulator to offer SSL-encrypted 3270 or 5250 sessions, which would make a frame trace reconstruction of user data virtually impossible. This was first offered with Host On-Demand Version 4. With Host On-Demand Version 8, it is even possible to encrypt VT sessions.

In addition to the server authentication, where the client authenticates the server as valid, client authentication is also available. By enabling client authentication, Host On-Demand can be restricted to only those clients with a valid certificate.

Host On-Demand also has additional functions that build on top of the SSL-enablement: Native Authentication, Certificate Express Logon and Telnet-negotiated sessions. While these are not security functions, they build on the security already in Host On-Demand and can make a secure environment easier for the end user and the administrator. Here are the security functions available in Host On-Demand client:

- Delivery of the HTML, applets, and preferences through HTTPS
- SSL-enabled host sessions (native TN3270, TN5250, VT or FTP)
- Client authentication (requires the user to have a digital certificate recognized by the Telnet server)
- Telnet-negotiated security, the ability to negotiate a secure connection over the same port as a non-secure Telnet session (see 11.13, “Telnet-negotiated session” on page 468)
- Certificate Express Logon requires SSL session with client authentication, and automatically logs the user into the zSeries host application without any additional prompts (see 15.2, “Certificate Express Logon” on page 580).)
- SSH-enabled VT or sftp sessions

Each has certain infrastructure requirements that must be met. In deciding how much security is “enough,” the security needs must be balanced with the infrastructure and administrative requirements.

Using a separate Host On-Demand and/or Telnet server for high-security users is also a common solution for extranet and Internet environments. The security policies of many companies prohibit a direct connection from the Internet to their mainframe business systems. These companies establish servers in a secure segment of their network called the demilitarized zone (DMZ) that provides a buffer between the Internet and the operational systems inside. With Host On-Demand, the same security principles apply. So, a Host On-Demand server is set up inside the DMZ to serve extranet and Internet users. Usually, this is an SSL-based (HTTPS) Web server. Access to this server is usually restricted by some form of logon, with direct access first being authenticated by a gateway server of some kind.

If a Host On-Demand server is placed within a DMZ, then a Telnet server is the next requirement. The placement of a Telnet server within a DMZ is one solution. Having SSL enabled on the Telnet server is required in order to make it secure. As an alternative, Telnet traffic can also be redirected through the firewall through proxy servers, the Host On-Demand Redirector (only for low-volume traffic) or by using the Telnet proxy function of the IBM Communications Server for AIX or Linux.

The final stop for Host On-Demand security is the target host itself. Generally, these are well-protected machines with highly evolved security mechanisms such as RACF. At this point, it is the user that becomes the weakest link in the chain. It is distinctly possible that in order to get to a host application, an extranet user may have to know:

- A user ID and password to an external Web site
- A Host On-Demand user ID and password
- A RACF user ID and password
- In some cases, it is possible that users may even have to log on to individual applications.

A user faced with this gauntlet is likely to record this information somewhere: a spreadsheet, a text file or even the famous yellow sticky on the display terminal or under the keyboard.

13.3.1 Firewall considerations

When you allow external users outside your company intranet access to Host On-Demand and Host On-Demand's emulator capabilities, you need to configure your company's firewall to allow for this remote access. You will need at least one port, the Telnet port, to be open on the firewall. The Host On-Demand configuration server port is optional.

If you do not use the configuration servlet (see Chapter 9, "Configuration servlet" on page 387), port 8999 on the firewall must be opened and directed to the Host On-Demand server port 8999. This port is only needed if you are using the Configuration Server-based model, License User Management (LUM) or Combined Server model. See 13.1, "Host On-Demand configuration models" on page 502.

A firewall is your gateway from the Internet to the intranet for Host On-Demand users on the Internet side of the firewall. Remember to configure your Host On-Demand clients to use either the IP address of your firewall, or the DNS name of your firewall when setting the destination address for the emulator session. This is because the firewall blocks access to your internal IP addresses. For example, see Figure 13-5.

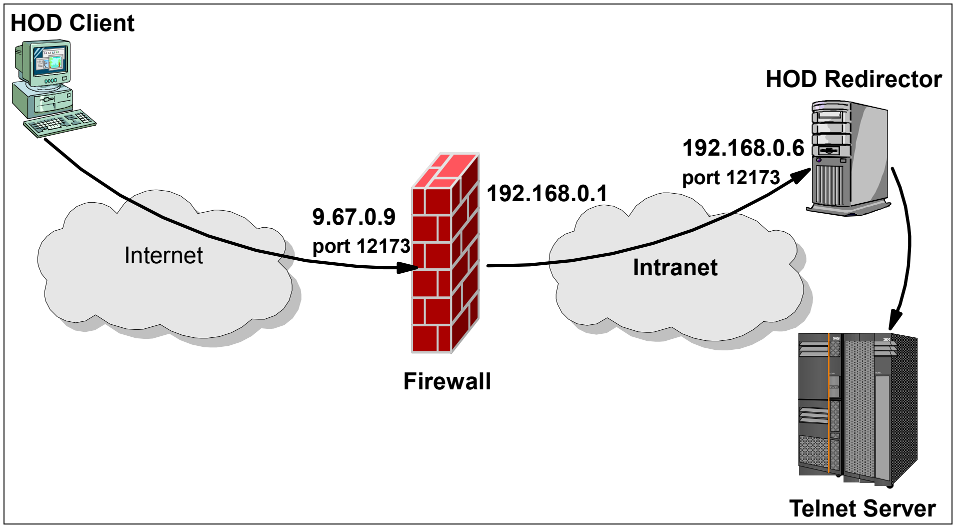


Figure 13-5 Network with firewalls

The IP address for your Host On-Demand Redirector is 192.168.0.6 using port 12173 on the company intranet. The firewall address is 9.67.0.9 on the Internet. The destination address for the Host On-Demand sessions is 9.67.0.9 and port 12173.

The firewall must be set up to forward all traffic that comes to it on port 12173 to 192.168.0.6 port 12173.

If you do not configure the firewall and Host On-Demand clients properly, the Host On-Demand clients will *not* connect to your intranet resources.

13.4 Host On-Demand server platform choices

Host On-Demand server code is designed to be platform independent, needing little more than a standard Java Runtime Environment and a Web server to provide its function. However, with the introduction of such features as Native Authentication, Certificate Express Logon, and support for Portal Server, the choice of server platform may be determined by the desire to use such features.

With Host On-Demand, the choice of the server platform is influenced by a combination of factors including:

- Number of Host On-Demand clients
- Reliability and availability requirements
- Security

- User location

If you have a large client base and users which require 24 x 7 access to the configuration server, these factors may influence the platform choice for the Host On-Demand server. Typically, installations with a large number of end users are installed on high availability systems such as UNIX-based platforms or the z/OS platform.

13.4.1 Security considerations

Security can dictate platform choice for Host On-Demand. There are two general factors that can influence platform choice with security. First is the use of Host On-Demand for extranet users. It is generally considered prudent to avoid having an extranet user with a direct Telnet connection from the Internet to a company's main systems. Given this rule, it is common practice to have a Host On-Demand server (with Telnet disabled) for extranet users running inside the company's DMZ. This server will usually run on either an Intel-based server (Windows NT or Windows 2000) or a UNIX server.

Even for a customer who will run Host On-Demand on a primary mainframe platform such as zSeries or iSeries, security concerns will often dictate the use of a second (distributed) platform.

Second, the use of the Host On-Demand Redirector to provide Telnet SSL can also dictate the use of the base platform for Host On-Demand. SSL is supported only on Windows NT and AIX Redirectors, and the use of SSL can impose a significant load on a server and must be considered carefully. Telnet negotiated security can also be used if connecting to a Telnet server that supports this option.

Third, the use of Host On-Demand's Native Authentication can also dictate the server platform choice. Native Authentication is dependent on the underlying operating system for validation of the user ID and password. If a company needs to validate Host On-Demand user IDs against RACF, that dictates deployment on a zSeries platform. Conversely, if a company wants to validate against a Windows NT domain structure, this would dictate deployment on a Windows NT server platform. Since Native Authentication is a Host On-Demand configuration Server deployment model, both cases would dictate a careful review of the need of registered Host On-Demand users.

13.5 User locations

Many of today’s businesses are global. Even smaller regional businesses often need to communicate with business partners or suppliers from around the country if not around the world. Also, today’s business world is very fluid; an environment where mergers and acquisitions are part of everyday life can result in some very interesting network campus arrangements. So, it is possible that geography can also play a large role in the Host On-Demand deployment strategy. In general, geography affects:

- Campus groupings
- WAN links
- Time zones
- Country (language) considerations

The first two factors are often interrelated. It is not unusual to find corporations spread across several major campuses that span their country or countries. Often each campus is serviced by individual “farms” of distributed systems. For example, a company that has offices in Philadelphia, Chicago, and San Francisco will likely use separate Windows NT domain servers at each site. Furthermore, it is not unusual to see larger distributed platforms (for example, UNIX and mainframe servers) at several locations. For example, a company may have offices in five locations in various places in the United States, but have major data centers in only two of the locations.

Given a company’s geographical situation, how can this affect their deployment of Host On-Demand? First, the geographical dispersion of the Host On-Demand user community needs to be taken into account when estimating the server size or possible traffic added by Host On-Demand clients accessing the Host On-Demand Server. IBM performance testing has indicated that Host On-Demand adds workload to a server under the following conditions:

- When a user logs on to a Host On-Demand server configured for LDAP or Native Authentication.
- During either the initial cached client download, or an update to the cached client, and for each invocation of the download client. The ability to tailor the client using componentization can significantly reduce the client download size, since only the required modules are downloaded.

The issue here is how the interactions between deployment choices and geography can impact Host On-Demand. In short, it is important to understand the geographical dispersion of users, since their use will skew the load on the Host On-Demand (and Telnet) server(s). For example, if a company is planning to support 3,000 total users, but they are spread across three time zones in four locations, due to the geographical constraints, it is likely the load on the server will be balanced for each time zone. Also, if the deployment choice is made to use a HTML-based configuration server model that does not require Host On-Demand users to logon to Host On-Demand server, then the load on the server will be similar to that of a normal Web server.

13.6 Other considerations

An additional environment worth mentioning is Microsoft Windows Terminal Services either separately or with Citrix Metaframe. It is possible to use Host On-Demand with this software, but keep in mind that running the Host On-Demand server and cached client on the same machine is not supported in the Windows Terminal Server or Citrix Metaframe environment. Therefore, you can either install Host On-Demand on the Terminal Services server and have the users use the download client, or install Host On-Demand on a different machine and have the users use the Host On-Demand cached client. The last configuration is recommended.

14

Deployment Wizard

The Deployment Wizard is a tool that is used by the administrator to create and edit customized HTML files. These files can contain a variety of information, depending on the options specified in the Deployment Wizard. The customized files are read by the applet that is downloaded to clients.

This tool is a Java application that runs only on a Windows platform. It is automatically installed when you install Host On-Demand server on a Windows system. Beginning with Host On-Demand V67, the Deployment Wizard can be installed as a stand-alone program on a Windows platform. The stand-alone Deployment Wizard can be installed from either a Host On-Demand for Windows CD or by downloading the image from the Host On-Demand server. The resulting Deployment Wizard files can then be distributed to the system where Host On-Demand is installed.

Using the Deployment Wizard is not required for an end user to launch a session. A set of default HTML files is shipped with Host On-Demand and these can be used by the end user to launch a session, provided the administrator has previously used the Host On-Demand Administration Utility to configure a session for the end user. However, by using the Deployment Wizard the administrator is able to take of advantage of features such as selecting the client level of Java, and tailoring the Host On-Demand applet size.

14.1 Planning

Some users and administrators may need to use customized HTML created by the Deployment Wizard, while others will find the default configuration HTML sufficient. To decide whether or not to use the Deployment Wizard, consider the following:

- Do you require end users to save their user preferences locally?
- Do you wish to select the level of client Java support?
- As the administrator would you like to tailor the download size of the applet to clients?
- Do you wish to create a customized HTML template to be used as the Host On-Demand Web page?
- Do you wish to modify the default port specified at install time to communicate with the Configuration Server?

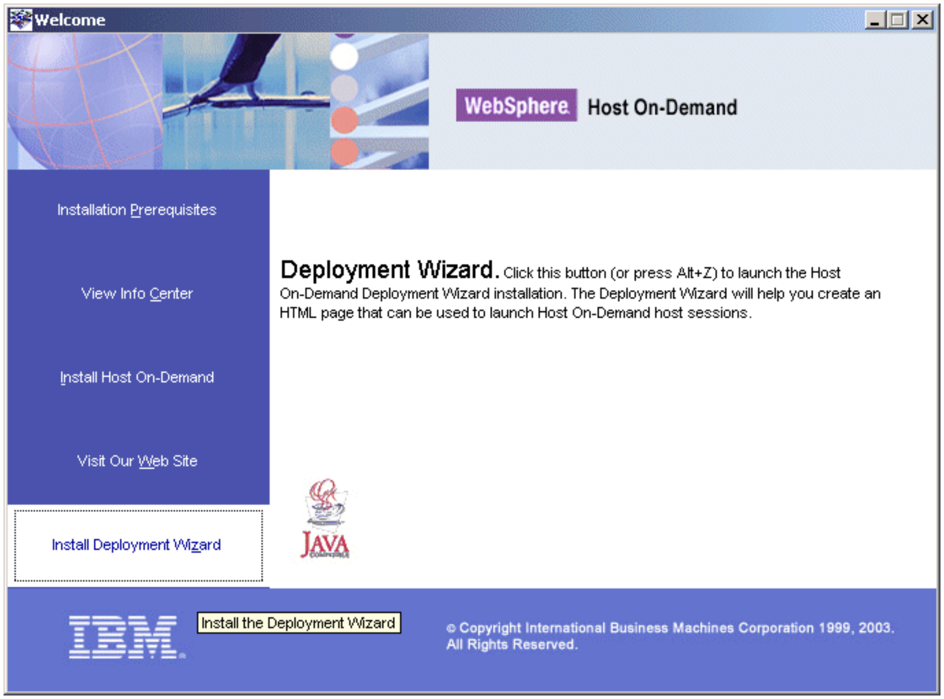
If the answer to any of the above is yes, you should consider using the Deployment Wizard to create custom HTML files.

See 2.4.9, “Installing the Deployment Wizard” on page 53, for details on installing the Deployment Wizard.

14.2 Starting the Deployment Wizard

If you have installed Host On-Demand on a Windows platform start the Deployment Wizard by selecting **Start -> Programs -> IBM Host On-Demand -> Administration -> Deployment Wizard.**

To install the stand alone Deployment Wizard, insert the Host On-Demand Windows/AIX installation CD then click **Install Deployment Wizard** from the Host On-Demand Welcome window as shown in Figure 14-1.

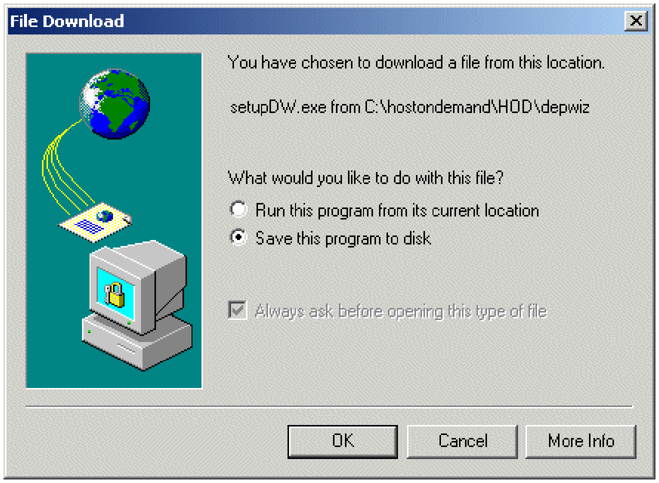


Deployment Wizard. Click this button (or press Alt+Z) to launch the Host On-Demand Deployment Wizard installation. The Deployment Wizard will help you create an HTML page that can be used to launch Host On-Demand host sessions.

© Copyright International Business Machines Corporation 1999, 2003. All Rights Reserved.

Figure 14-1 Host On-Demand Welcome

The Deployment Wizard can also be downloaded from your Host On-Demand server. Start your browser and point to the `HODMain.html` page. Click **Deployment Wizard Installation Image for Windows** on the administrator's page to download the file to your workstation. From the File Download window click **OK** to save the file to your workstation (see Figure 14-2).


File Download

You have chosen to download a file from this location.

setupDW.exe from C:\hostondemand\HOD\depwiz

What would you like to do with this file?

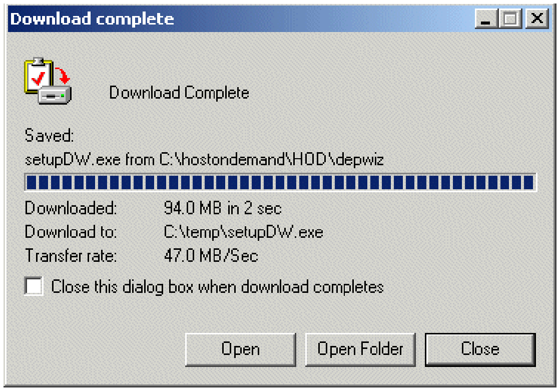
○ Run this program from its current location

● Save this program to disk

☑ Always ask before opening this type of file

Figure 14-2 Deployment Wizard download

After saving setupDW.exe you can either run the program from the window as shown in Figure 14-3 or run **`setupDW.exe`**.


Download complete

Download Complete

Saved:
setupDW.exe from C:\hostondemand\HOD\depwiz

Downloaded: 94.0 MB in 2 sec
Download to: C:\temp\setupDW.exe
Transfer rate: 47.0 MB/Sec

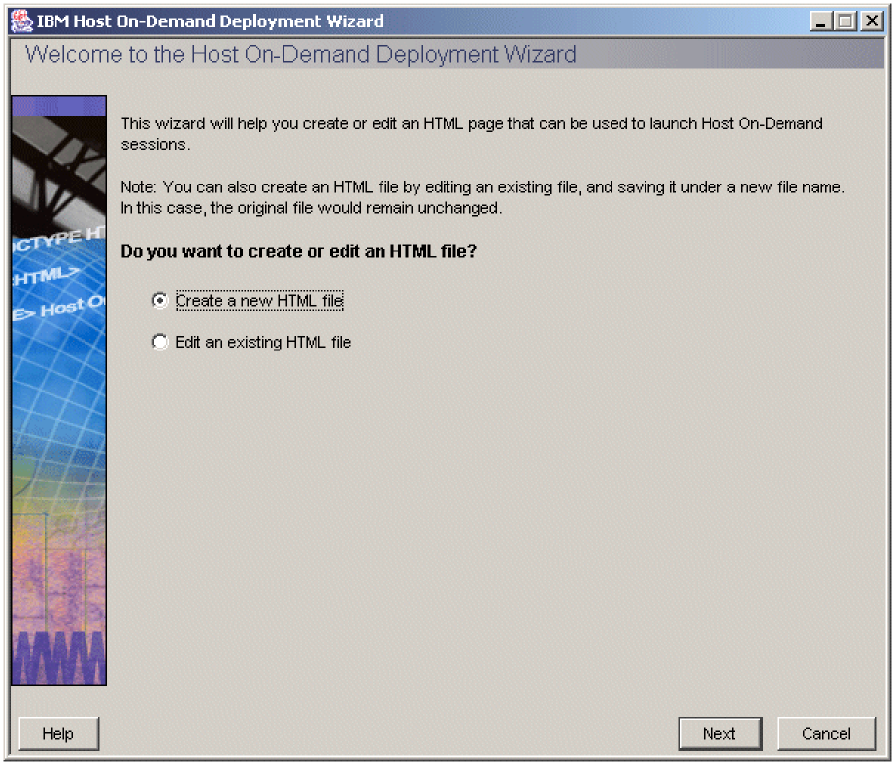
□ Close this dialog box when download completes

Figure 14-3 Deployment Wizard installation

Once installation is complete, launch the Deployment Wizard from the **Start > Programs** desktop menu.

14.3 Using the Deployment Wizard

After starting the Deployment Wizard, the Welcome to the Host On-Demand Deployment Wizard window is displayed as shown in Figure 14-4.



Welcome to the Host On-Demand Deployment Wizard

This wizard will help you create or edit an HTML page that can be used to launch Host On-Demand sessions.

Note: You can also create an HTML file by editing an existing file, and saving it under a new file name. In this case, the original file would remain unchanged.

Do you want to create or edit an HTML file?

● Create a new HTML file

○ Edit an existing HTML file

Figure 14-4 Deployment Wizard Welcome

The default setting is Create a new HTML file. If you want to edit existing HTML files that were created by the Deployment Wizard, select **Edit an existing HTML file**. It is recommended that you do *not* manually edit files created by the Deployment Wizard, nor should you use the Deployment Wizard to edit files that it did not create; doing so can render the file unusable.

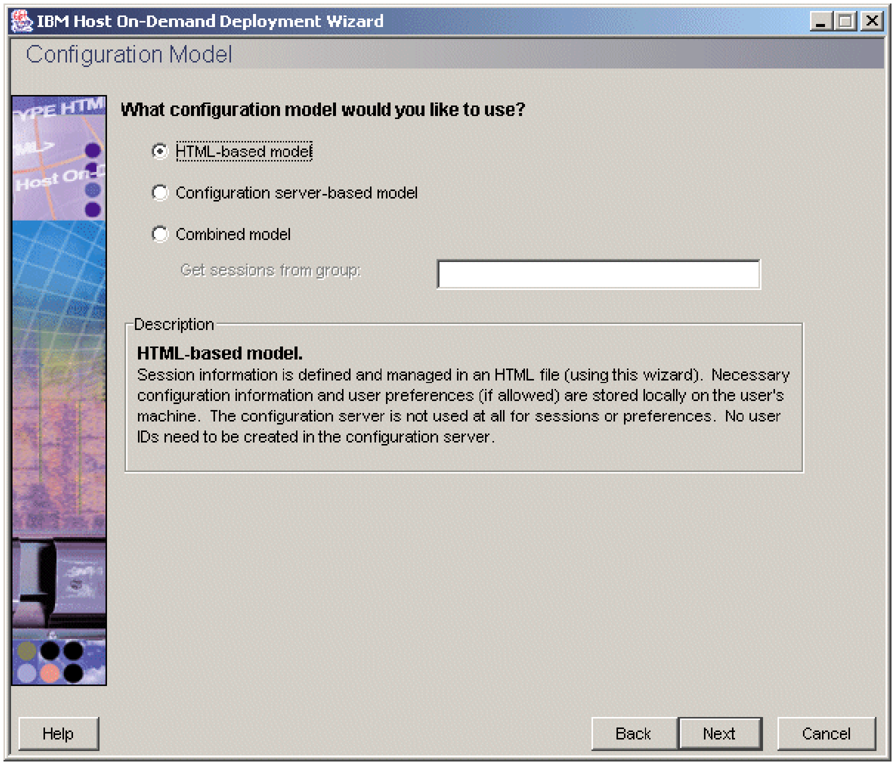
If the server is on an iSeries system, see 4.7.4, “Mapping a network drive to the iSeries” on page 145. A network drive connection allows custom HTML files to be opened and updated using the Deployment Wizard.

We will now demonstrate the use of the Deployment Wizard with an example illustrating how to create a custom HTML page for each of the configuration models.

14.3.1 HTML-based model example

With the HTML-based model, the administrator does not have to log on to the configuration server to create or maintain Host On-Demand user IDs. All host session configuration information is contained in the files created by the Deployment Wizard. If the administrator allows users to save changes to their host session configuration settings (such as keyboard remappings) changes are stored on the user's local file system.

A description of the selected model is displayed in the center of the window as shown in Figure 14-5.



What configuration model would you like to use?

● HTML-based model

○ Configuration server-based model

○ Combined model

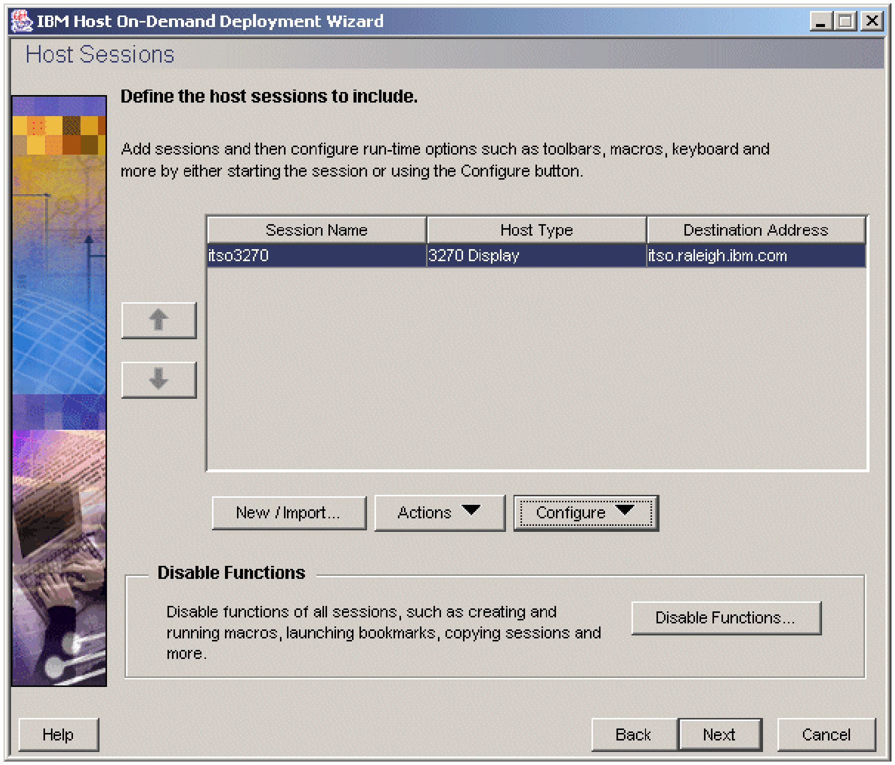
Get sessions from group:

Description

HTML-based model.
Session information is defined and managed in an HTML file (using this wizard). Necessary configuration information and user preferences (if allowed) are stored locally on the user's machine. The configuration server is not used at all for sessions or preferences. No user IDs need to be created in the configuration server.

Figure 14-5 HTML-based model

Clicking **Next** will display the Host Sessions window. For this scenario, the administrator defines a basic 3270 session with a session name of itso3270, specifies the destination address, and clicks **Add**. This adds the session to the table as shown in Figure 14-6.


IBM Host On-Demand Deployment Wizard

Host Sessions

Define the host sessions to include.

Add sessions and then configure run-time options such as toolbars, macros, keyboard and more by either starting the session or using the Configure button.

Session Name	Host Type	Destination Address
itso3270	3270 Display	itso.raleigh.ibm.com

Disable Functions

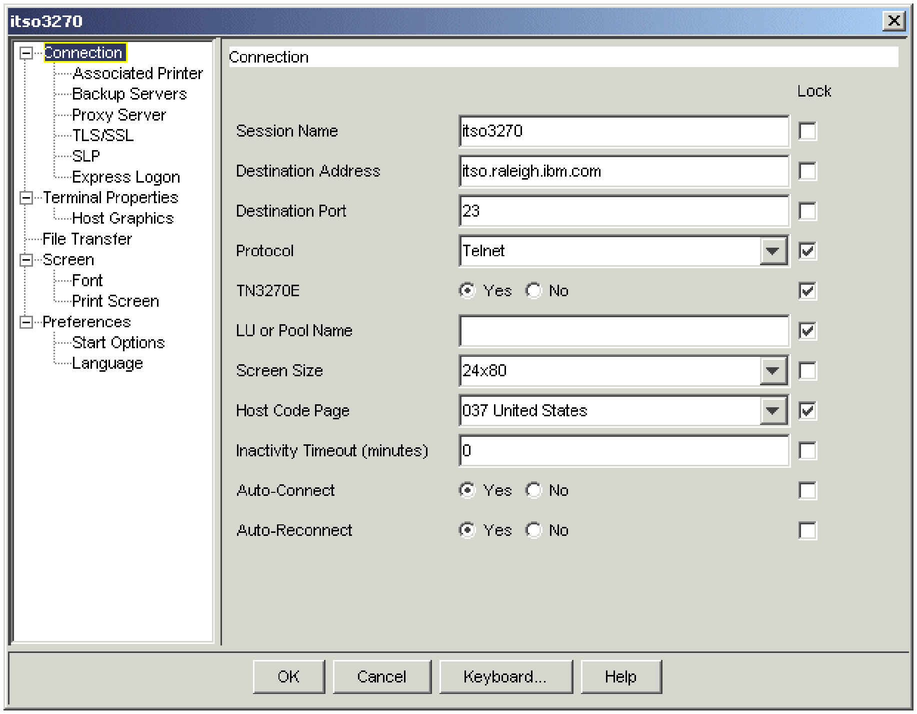
Disable functions of all sessions, such as creating and running macros, launching bookmarks, copying sessions and more.

Figure 14-6 Host Sessions

More than one session can be added to the table if the administrator wants to provide access to other systems. A session icon will be created on the end user's client window for each session defined. If more than one session is created, icons can be re-ordered by highlighting the session and clicking the up or down arrow. However, once a user has accessed the HTML page the initial order will override subsequent changes made by the administrator.

Note: It is possible to add a very large number of sessions, but there can only be a maximum of 26 sessions opened concurrently by a single user. This number can be further limited by the Maximum number of concurrent sessions per user field on the Advanced Options window (see Figure 14-14 on page 532).

To set a session's configuration properties, highlight the session and click **Configure** -> **Properties** or double click the list entry. This will display a properties window unique to the type of session being defined. For a 3270 Display session, the window shown in Figure 14-7 is displayed.



Connection

		Lock
Session Name	itso3270	☐
Destination Address	itso.raleigh.ibm.com	☐
Destination Port	23	☐
Protocol	Telnet	☑
TN3270E	● Yes ○ No	☑
LU or Pool Name		☑
Screen Size	24x80	☐
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)	0	☐
Auto-Connect	● Yes ○ No	☐
Auto-Reconnect	● Yes ○ No	☐

Figure 14-7 Session properties

This window is similar to the window described in 7.1.7, “Configuring sessions” on page 277 where the fields are described in detail. The Deployment Wizard online help provides a description of each field. The online help also details fields and selections that have been added in Host On-Demand Version 8 such as the `Proxy Server selection` (refer to “3270/5250 Proxy Server selection” on page 288). Note that some fields are locked by default, for example, the Destination Address and Destination Port fields. It is recommended to lock these fields because if they are altered by a user they could affect the operability of the session. Administrators, however, may change these settings if they desire.

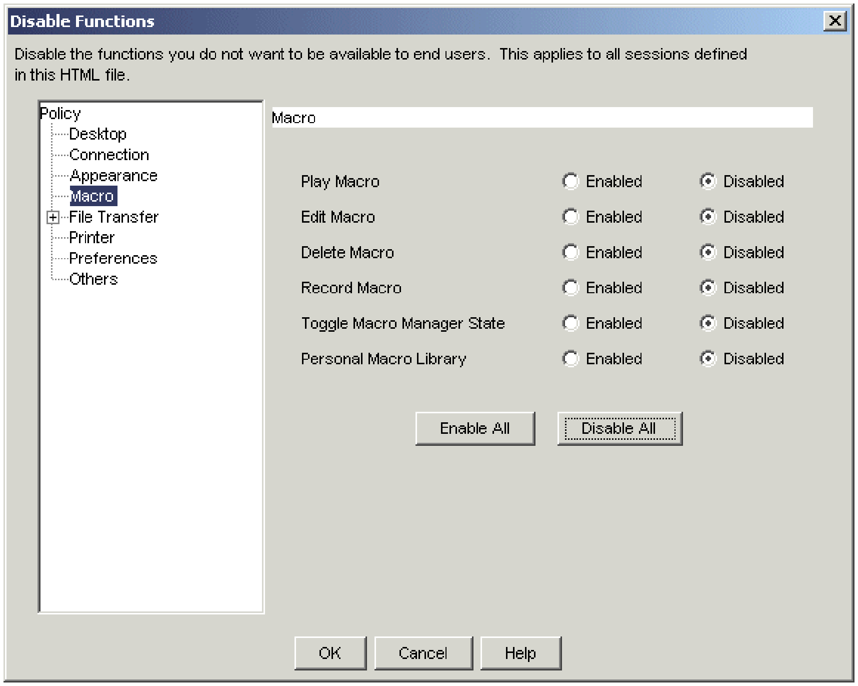
After configuring the session properties and clicking **OK**, control is returned to the Host Sessions window shown in Figure 14-6 on page 523.

The administrator can provide initial settings for runtime options (such as color or key remappings and screen size), by clicking **Actions** -> **Start**. Doing so will start the host session, verify connectivity for the session, and allow the administrator to alter the runtime options. After the runtime options are modified, the administrator will close the session, storing the preferences. These preference settings will apply only to the highlighted session. For this scenario, the settings will not be modified.

Clicking **Actions** -> **Copy** will copy the highlighted session creating a new session. The new session will have the name *n*`:xxxxx`, where *n* is an integer beginning with 1 and `xxxxx` is the name of the original session. When a session is copied, the session configuration attributes are copied as well as the runtime options.

Clicking **Actions** -> **Delete** will remove a session from the table and all of its associated configuration data.

Clicking **Disable Functions** allows the administrator to restrict selected functions from the end users. In this scenario, the administrator is disabling all macro functions as shown in Figure 14-8. Disabling a function prevents the client from being able to view the function.



Disable Functions

Disable the functions you do not want to be available to end users. This applies to all sessions defined in this HTML file.

Macro

Play Macro ○ Enabled ● Disabled

Edit Macro ○ Enabled ● Disabled

Delete Macro ○ Enabled ● Disabled

Record Macro ○ Enabled ● Disabled

Toggle Macro Manager State ○ Enabled ● Disabled

Personal Macro Library ○ Enabled ● Disabled

Figure 14-8 Disable functions

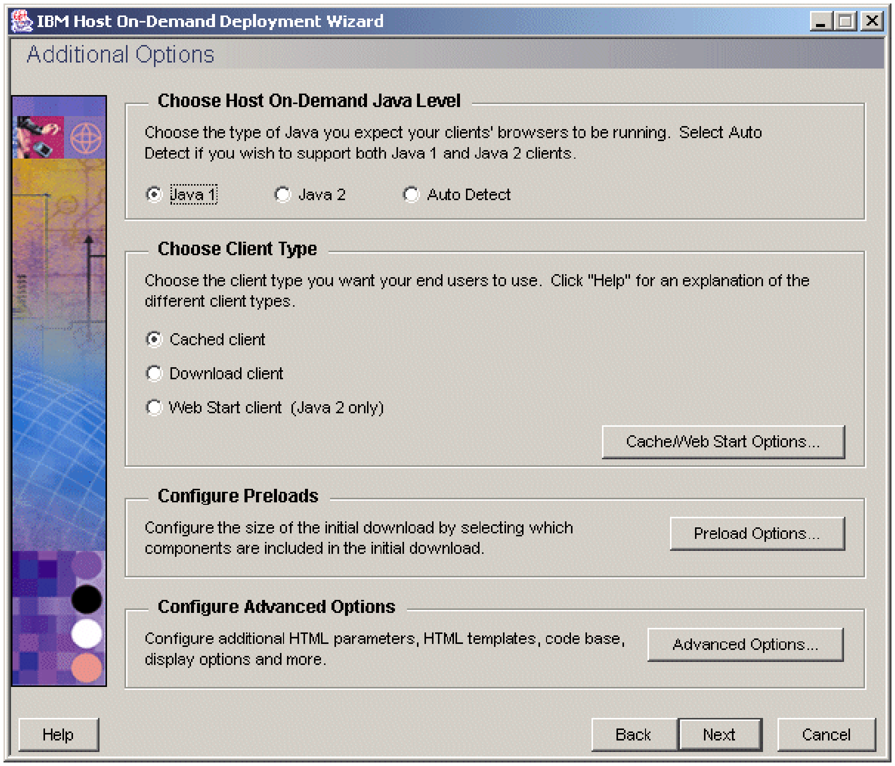
Select the various policy categories to locate and mark the functions you will disable. Click **OK** to return.

> **Note:** Disabling functions applies to *all* sessions defined in the HTML file, not just the highlighted one.

Disabling functions is different from locking specific fields. The administrator can lock fields when configuring a session. After that the users will not be able to change the values for those fields. If the user displays the session properties, these fields will appear in gray. When a function is disabled, it is removed from the toolbar or menus so users will not even see it.

Details on the ability to disable functions are also found in the Administration Utility; see 7.1.8, “Disabling functions” on page 334.

To continue, click **Next** on the Host Sessions window and the Additional Options window shown in Figure 14-9 is displayed.



IBM Host On-Demand Deployment Wizard

Additional Options

Choose Host On-Demand Java Level

Choose the type of Java you expect your clients' browsers to be running. Select Auto Detect if you wish to support both Java 1 and Java 2 clients.

● Java 1 ○ Java 2 ○ Auto Detect

Choose Client Type

Choose the client type you want your end users to use. Click "Help" for an explanation of the different client types.

● Cached client

○ Download client

○ Web Start client (Java 2 only)

Configure Preloads

Configure the size of the initial download by selecting which components are included in the initial download.

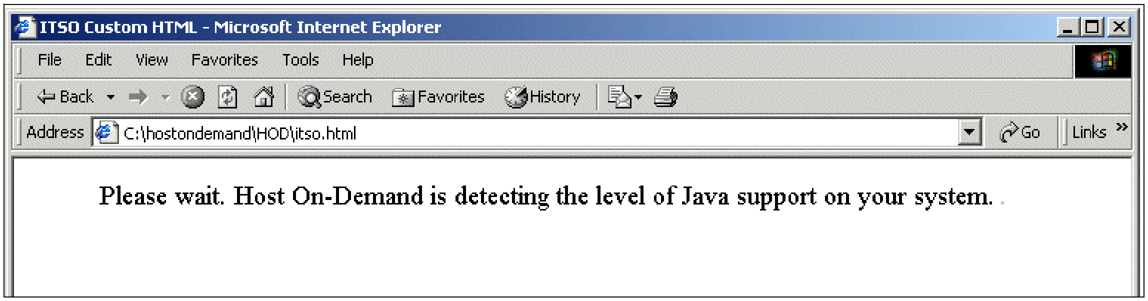
Configure Advanced Options

Configure additional HTML parameters, HTML templates, code base, display options and more.

Figure 14-9 Additional options

This window has multiple functions.

First the administrator can select Java 1 (the default), Java 2 or Autodetect in the Client Java Type field. The value in this field refers to the Java level in the client's browser. When Autodetect is selected, end users will experience a delay while Host On-Demand attempts to detect if a Java 2 plug-in is available. A message will be displayed as shown in Figure 14-10.


ITSO Custom HTML - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\hostondemand\HOD\itso.html
Go Links

Please wait. Host On-Demand is detecting the level of Java support on your system.

Figure 14-10 Java detect

Note: The autodetect process checks for a installed Java 2 environment only, not whether it is active, or whether the browser is configured to use it.

If your end users only have Java-1 enabled browsers, we recommend that you use the default setting which will bypass the detection process. If your end users are all using Java-2 enabled browsers select **Java 2**. If you are unsure of the level of Java in the end user's browser or have both Java 1 and Java-2 clients then select **Autodetect**. For more information see 5.9, "Java 2 support" on page 179.

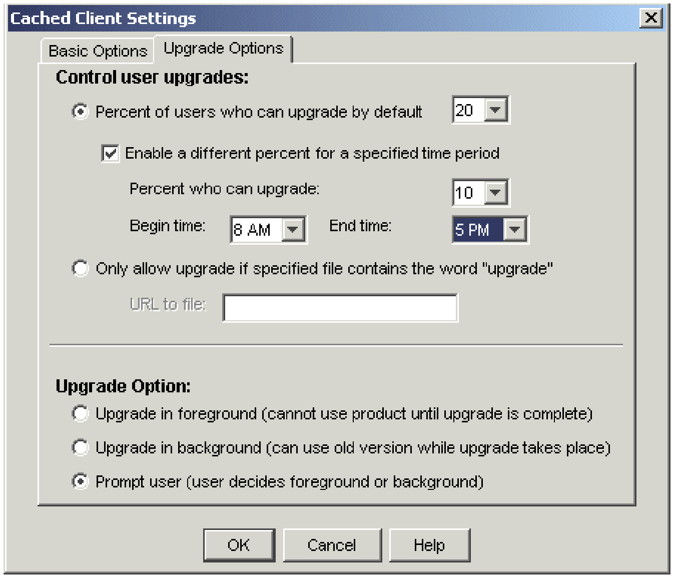
The next section of the window lets the administrator determine if a cached, downloaded or Web start client will be created. If the cached client is selected, clicking **Cache/Web Start Options** will further tailor the caching process. The administrator can select some load-balancing techniques that handle mass downloads when an upgrade is available, and whether to allow the update to happen in the foreground or background. In Host On-Demand Version 8 the administrator can restrict the number of users that can upgrade in a certain time period. Note that Cache options are only valid if you are upgrading from Host On-Demand Version 5 or higher.

In this scenario, on the Cache Client Upgrade Option tab, shown in Figure 14-11, the administrator specifies that 20% of the users can upgrade, however, only 10% of users can upgrade from 8am to 5pm. Specifying a percentage during a time period enables the administrator to control the amount of network traffic during their peak business hours.

If the administrator selects less than 100% in the `Percent of users who can upgrade by default` field, the administrator will need to re-edit the HTML file at a later stage to increase the percentage. This is required to ensure that all end users are upgraded. For example, in Figure 14-11 the administrator enters 20% as the `Percent of users who can upgrade by default`. The Host On-Demand applet randomly allocates a number which is used to determine if a user can upgrade. It is possible that even after accessing the HTML page several times a user may still not be upgraded. The initial percentage of users who can upgrade and the rate of increase will depend on your network infrastructure. For example, the administrator initially selects **20%**. In this scenario, users access the Host On-Demand page daily and after a week the administrator is advised that the majority of users have been upgraded. The administrator re-edits the HTML file and modifies the upgrade percent to `100` to ensures all the remaining users will be upgraded.

The administrator can select whether the upgrade can take place in the foreground or background, where it will not disrupt the current open session. In this scenario the administrator will allow the end user to decide as shown in Figure 14-11. Note that selecting **Upgrade in foreground** will freeze the end users window until the download is complete, hence, this option is not recommended if your end users have low speed connections to the server such as dial-up connections.

.



Control user upgrades:

● Percent of users who can upgrade by default: 20

☑ Enable a different percent for a specified time period

Percent who can upgrade: 10

Begin time: 8 AM End time: 5 PM

○ Only allow upgrade if specified file contains the word "upgrade"

URL to file:

Upgrade Option:

○ Upgrade in foreground (cannot use product until upgrade is complete)

○ Upgrade in background (can use old version while upgrade takes place)

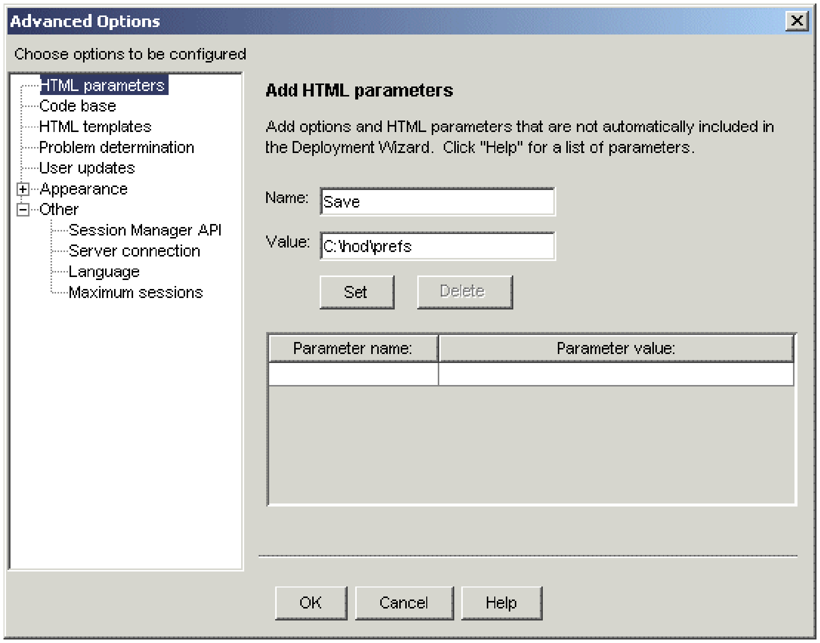
● Prompt user (user decides foreground or background)

Figure 14-11 Cache options

Restriction: Java 2 cached clients cannot upgrade in the background when migrating from HOD 7 to HOD 8.

After specifying the cache options click **OK** to return to the Additional Options window shown in Figure 14-9 on page 526.

Clicking **Advanced options** -> **HTML parameters** brings up the selection shown in Figure 14-12, which allows administrators to set some additional parameters to be passed to Host On-Demand that will apply to the HTML files being created. The values specified for the parameters in the HTML file take precedence over the values that may be specified in the config.properties file.



Add HTML parameters

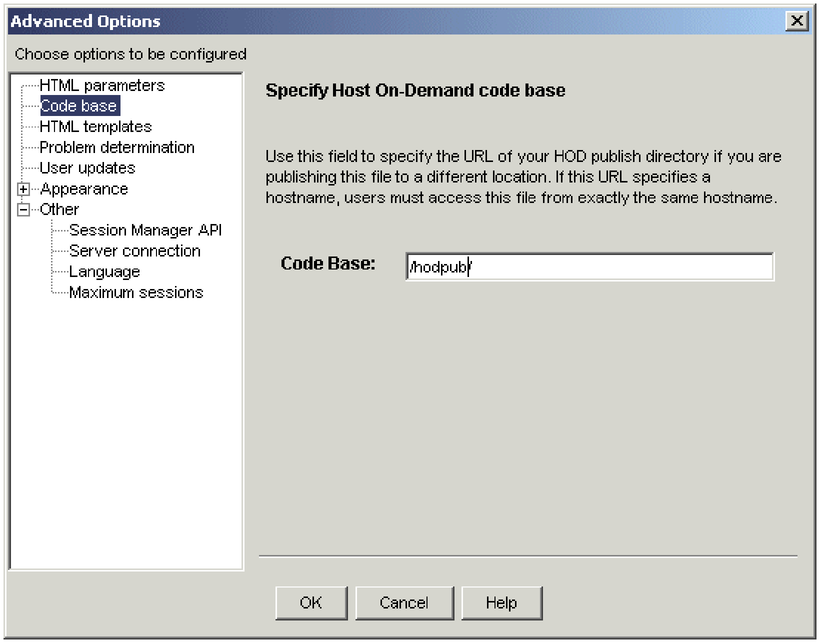
Add options and HTML parameters that are not automatically included in the Deployment Wizard. Click "Help" for a list of parameters.

Name: Save

Value: C:\hod\prefs

Figure 14-12 HTML parameters selection

Clicking the **Code base** selection on the Advanced Options panel brings up the window as shown in Figure 14-13. In Host On-Demand Version 8 administrators can publish files generated from the Deployment Wizard to a location other than the Host On-Demand server publish directory. This function makes future upgrades easier and allows system administrators to restrict access to the publish directory. In this scenario the administrator selects to use this feature, and enters the alias for the Host On-Demand publish directory in the Codebase field as shown in Figure 14-13.



Specify Host On-Demand code base

Use this field to specify the URL of your HOD publish directory if you are publishing this file to a different location. If this URL specifies a hostname, users must access this file from exactly the same hostname.

Code Base: /hodpub/

Figure 14-13 Code base selection

In this example a relative path has been entered. You can also enter a fully qualified URL in the Codebase field. Note that if you use a fully qualified URL, the Web server name must match exactly with what the user enters in their Web browser, even if the DNS entries resolve to the same IP address. For example, the administrator enters the Codebase field as follows:

```
http://itsoweb.raleigh.ibm.com/hodpub/
```

The customized HTML file created by the administrator is called itso.html. In this example we will assume that itsoweb.raleigh.ibm.com and webhod8.ibm.com resolve to the same IP address. If a user enters the following on their browser it will fail as the server DNS names do not match.

```
http://webhod8.ibm.com/hodpub/itso.html
```

In a like manner if you use an IP address in the fully qualified URL, the client cannot use a DNS name in their browser URL. We recommend using a relative URL if possible as it also provides the ability to load balance across multiple Host On-Demand servers.

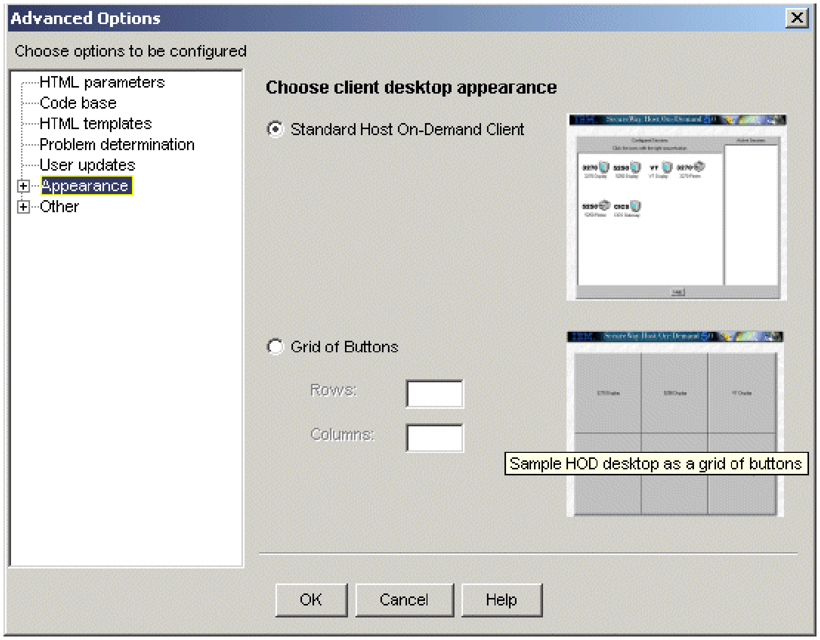
Important: The Codebase parameter refers to the installed Host On-Demand server publish directory, not the directory where you will publish the Deployment Wizard files.

In Host On-Demand Version 8, the administrator can choose to select a customized HTML template they have previously created. This is configured at the **HTML templates** selection. For more information on Customizing HTML templates see Chapter 17, “Custom HTML templates” on page 615.

The **User updates** selection allows the administrator to specify whether an end user can save user preferences, for example, keyboard re-mapping, made during an open session. If **No** is selected, end users are prevented from saving changes, ensuring that each time a session is opened, the original session properties are used. If **Yes** is selected, user changes will persist.

To reduce confusion, the administrator should inform the end users if saving changes is not allowed; otherwise, it may not be obvious to the end users why their changes are not being maintained from session to session. To control whether or not a user is allowed to make changes, use the Lock checkboxes found on the Session Properties window (see Figure 14-7 on page 524). It is possible for the administrator to let the end users change the values of a session (by not locking the fields) but disallow the saving of these changes by selecting **No** to Persist user changes on the Additional Options window. Browser considerations are detailed in 14.3.4, “User preferences stored on local machines” on page 544. For this scenario, the administrator is allowing users to save changes.

The **Appearance** selection of the **Advanced Options** panel brings up the window shown in Figure 14-14. The Display window allows the administrator to select the format of the sessions displayed to end users



Advanced Options

Choose options to be configured

- HTML parameters
- Code base
- HTML templates
- Problem determination
- User updates
- Appearance
- Other

Choose client desktop appearance

● Standard Host On-Demand Client

○ Grid of Buttons

Rows:

Columns:

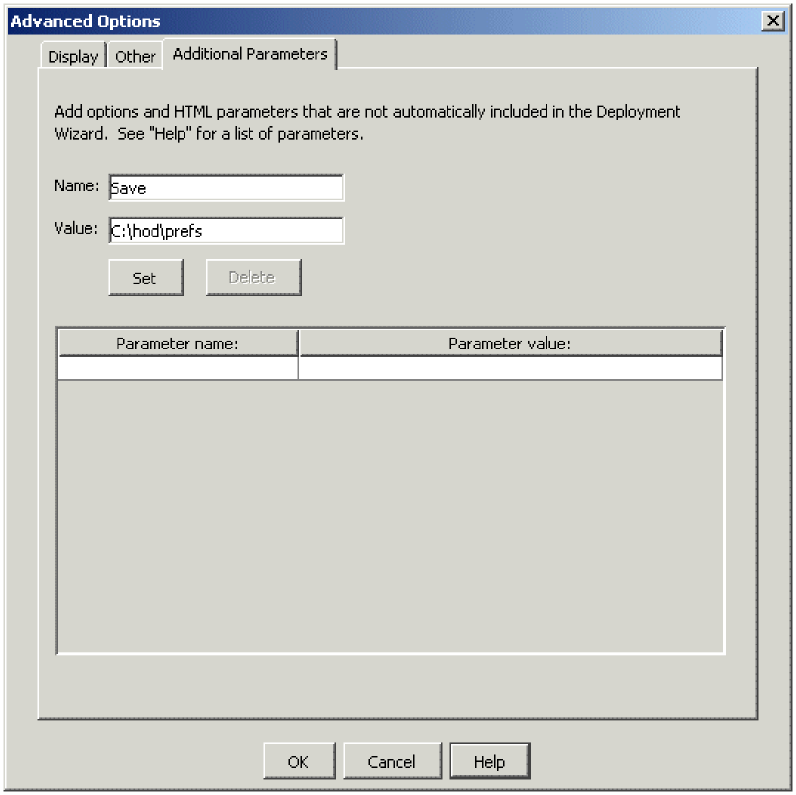
Sample HOD desktop as a grid of buttons

Figure 14-14 Appearance selection

The **Other** -> **Maximum sessions** selection lets the administrator define the number of open sessions allowed per user. In this scenario, we assume that the administrator restricts the number of open sessions per user to 5.

In this scenario we have altered the directory where local preferences will be saved by setting the `Save` parameter as shown in shown in Figure 14-15. See the online help or "Additional parameters" on page 551 for more HTML parameters allowed.

.



Advanced Options

Display | Other | Additional Parameters

Add options and HTML parameters that are not automatically included in the Deployment Wizard. See "Help" for a list of parameters.

Name: Save

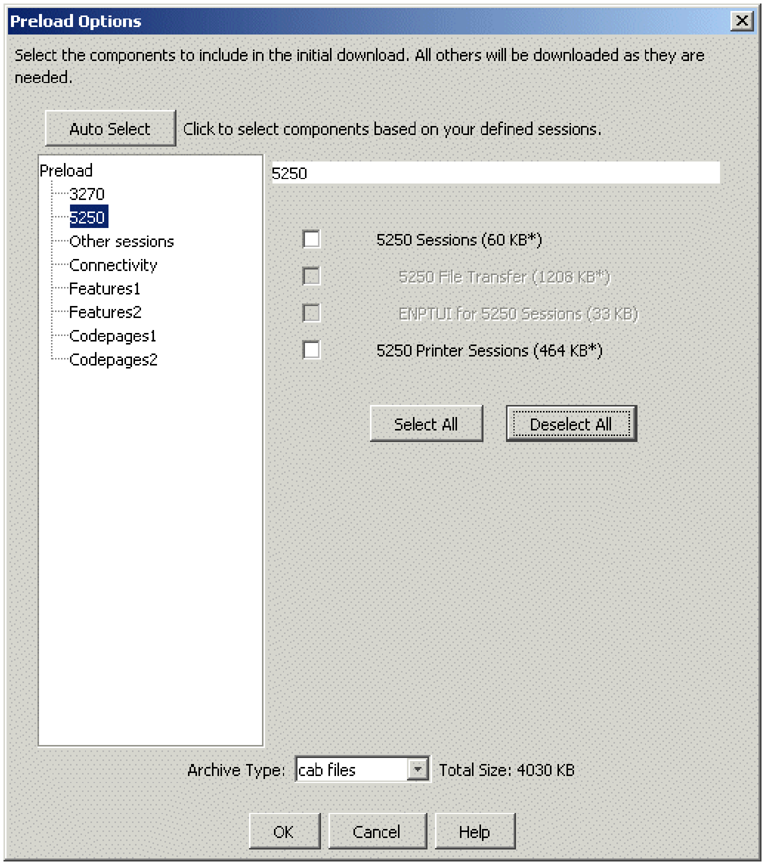
Value: C:\hod\prefs

Figure 14-15 Additional parameters

Click **Set** and then **OK** to return to the Additional Options window shown in Figure 14-9 on page 526.

Clicking **Preload Options** from the Additional Options window allows the administrator to select components which will be downloaded when the HTML file is accessed. By default everything, except for specific language code pages is downloaded. To reduce the size and time of the download, the administrator might choose to exclude certain components.

In this example, it is expected that the end users will only be using 3270 display/printer sessions. Therefore, to reduce the size of the download, the administrator clicks **Deselect All** on the 5250 display as shown in Figure 14-16. If these functions are ever needed by the end user, they will be downloaded upon subsequent access.



Preload Options

Select the components to include in the initial download. All others will be downloaded as they are needed.

Auto Select — Click to select components based on your defined sessions.

- Preload
  - 3270
  - 5250
  - Other sessions
  - Connectivity
  - Features1
  - Features2
  - Codepages1
  - Codepages2

5250

- □ 5250 Sessions (60 KB*)
- □ 5250 File Transfer (1208 KB*)
- □ ENPTUI for 5250 Sessions (33 KB)
- □ 5250 Printer Sessions (464 KB*)

Archive Type: cab files Total Size: 4030 KB

Figure 14-16 Preload options

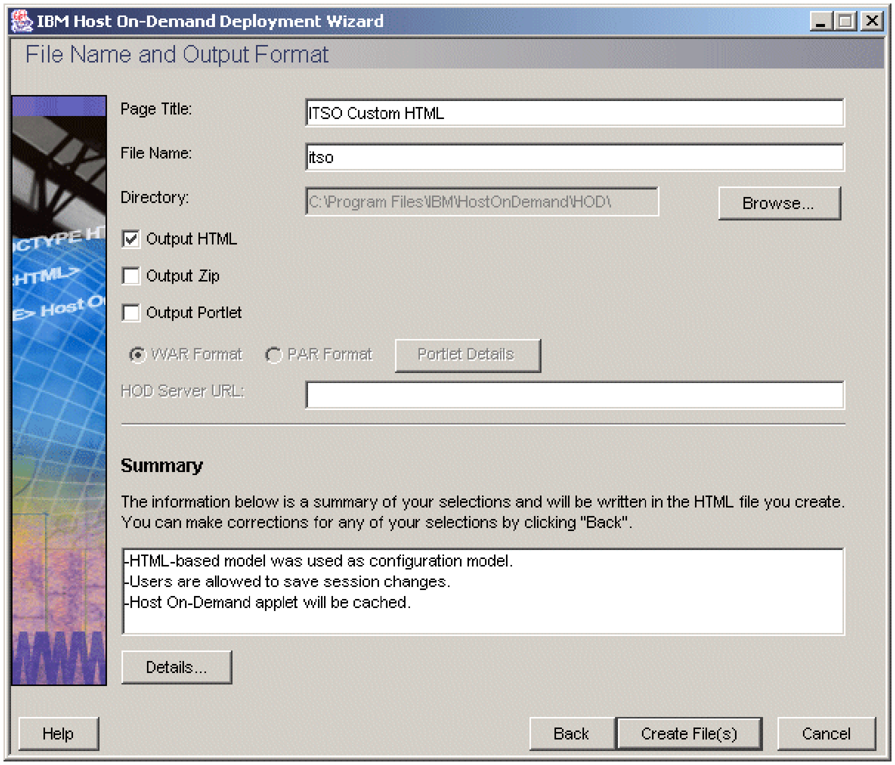
Restriction: If you are using the download client with a Java-2 enabled browser, functional components will not be downloaded as needed. You will need to ensure the preload component list contains all the components required by the client.

Some sessions share components, and selecting one but excluding another may not necessarily reduce the size of the download. For example, if the 3270 display session is excluded but the 3270 printer session is included, the size of the download is the same as if both were included, since the 3270 printer session needs some of the same files. In general, to reduce download size, select only those components that will be used. The preload options also apply when running the download client where the applet is downloaded every time the page is accessed, not just the first time.

Tip: When creating customized pages using the HTML model, you can use the **Auto Select** button. The Deployment Wizard will automatically select the components required based on the sessions configured and options checked.

After selecting the required download components, click **OK** to return to the Additional Options window shown in Figure 14-9 on page 526.

After completing the Additional Options window and clicking **Next**, the File Name and Output Format window is displayed as shown in Figure 14-17. This window displays a summary of the options selected thus far. The administrator supplies a page title, file name, and selects the directory where the Deployment Wizard output will be stored. If the Deployment Wizard is running on the server, the directory will be the Host On-Demand publish directory. The administrator can change the directory by clicking the on the **Browse** button to browse the file system. With Host On-Demand Version 7 and later, administrators can also select the type of output to be created by the Deployment Wizard. Output HTML is the default as shown in Figure 14-17. In this example the Deployment Wizard files will be created in C:\hostondemand\HOD.



File Name and Output Format

Page Title: ITSO Custom HTML

File Name: itso

Directory: C:\Program Files\IBM\HostOnDemand\HOD\

☑ Output HTML

□ Output Zip

□ Output Portlet

● WAR Format ○ PAR Format

HOD Server URL:

Summary

The information below is a summary of your selections and will be written in the HTML file you create.
You can make corrections for any of your selections by clicking "Back".

-HTML-based model was used as configuration model.
-Users are allowed to save session changes.
-Host On-Demand applet will be cached.

Figure 14-17 Wizard output

In Host On-Demand Version 8, administrators can choose to create a zip file by selecting **Output Zip**. This option creates a zip file of the Deployment Wizard-generated files. The DWunzip tool is used to install the files to the Host On-Demand server, see 14.4, “Distributing Deployment Wizard files” on page 547 for instructions. This format is recommended if you are running the Deployment Wizard on a different server or platform from your Host On-Demand server.

Host On-Demand Version 8 can run as a portlet on Portal Server, a component of IBM WebSphere Portal. If **Output Portlet** is selected, the administrator will need to configure additional parameters. See Chapter 19, “Host On-Demand portlets” on page 665 for further information on using Host On-Demand as a portlet.

Finally, the administrator selects **Create File(s)** and the Deployment Wizard output is created and stored in the specified directory. See 14.5, “Files created by the Deployment Wizard” on page 548 for a description of the files that are created.

If the Deployment Wizard is installed on a server different from the Host On-Demand server the files must be transferred to the system where Host On-Demand is installed. See 14.4, “Distributing Deployment Wizard files” on page 547 for instructions.

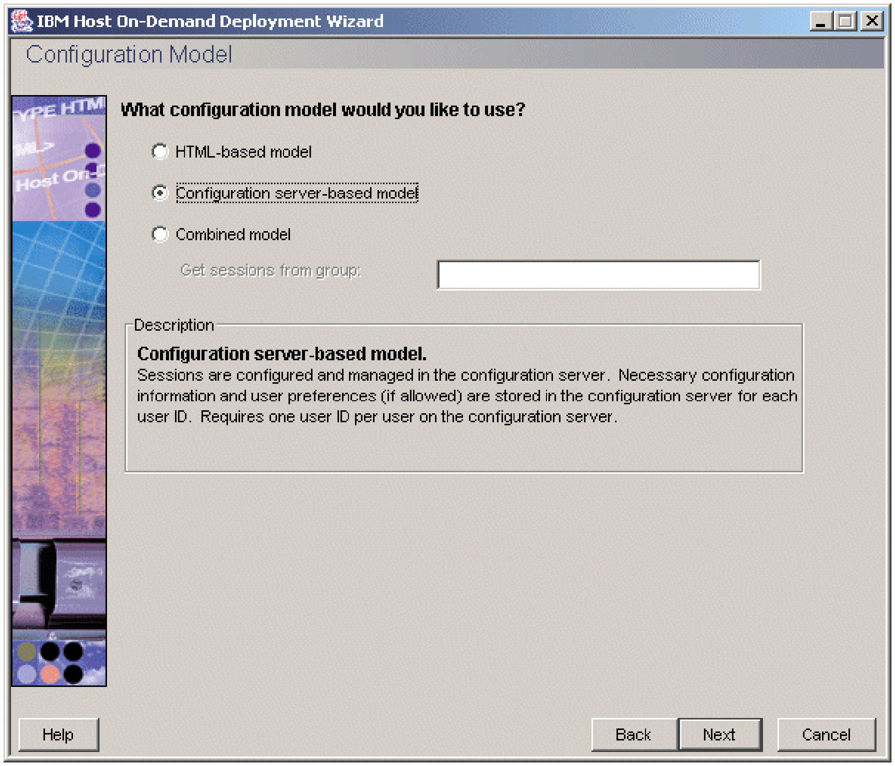
After the files have been distributed to the Host On-Demand server, end users will indicate the address of the machine where the Web server and Host On-Demand publish directory is installed, specifying the new customized HTML. For example:

```
http://TheHODWebserver/hod/itso.html
```

14.3.2 Configuration server-based model example

In the configuration server-based model, session information is maintained on the configuration server using the Host On-Demand Administration utility. Configuration information is defined in group or user IDs created by the administrator. If the administrator allows users to save preferences, changes are stored in the user ID on the server. This model can be useful in the scenario where clients access host sessions from a number of terminals, and they are unable to retrieve their local user preferences. With large number of users however there can be a high administrative requirement to create and maintain all the user IDs.

After starting the Deployment Wizard, and selecting **Create a new HTML file**, the administrator selects the **Configuration Server-based model** (see Figure 14-18).



What configuration model would you like to use?

○ HTML-based model

● Configuration server-based model

○ Combined model

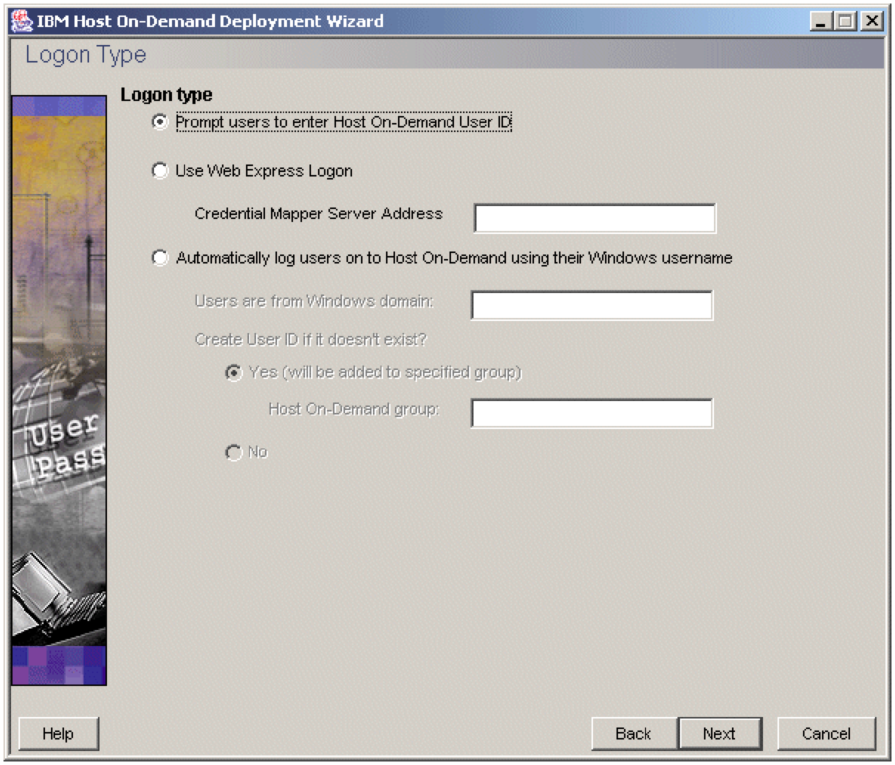
Get sessions from group:

Description

Configuration server-based model.
Sessions are configured and managed in the configuration server. Necessary configuration information and user preferences (if allowed) are stored in the configuration server for each user ID. Requires one user ID per user on the configuration server.

Figure 14-18 Configuration server-based model

The next window (shown in Figure 14-19) determines if the end users will log on using their Host On-Demand user IDs or their Windows user IDs. Since some of the users in this scenario may be on non-Windows platforms, the administrator chooses to use the Host On-Demand user IDs. This requires the administrator to set up user IDs using the Administration Utility prior to end users accessing the customized HTML page.



IBM Host On-Demand Deployment Wizard

Logon Type

Logon type

● Prompt users to enter Host On-Demand User ID

○ Use Web Express Logon

Credential Mapper Server Address

○ Automatically log users on to Host On-Demand using their Windows username

Users are from Windows domain:

Create User ID if it doesn't exist?

● Yes (will be added to specified group)

Host On-Demand group:

○ No

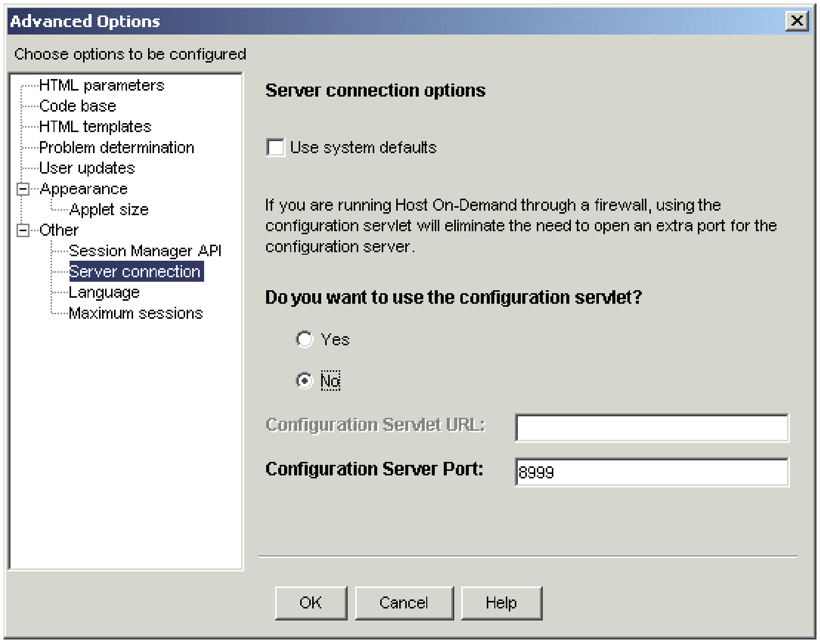
Figure 14-19 Logon type

If some of the end users run on the Windows platform and have similar connectivity requirements, the administrator may choose to group these users together and create a customized HTML file for them whereby they are automatically logged on to Host On-Demand using their Windows user ID. Using the Integrated Windows domain logon, Host On-Demand offers several advantages:

- Host On-Demand user IDs can be created automatically.
- Users can bypass the Host On-Demand logon window.

See 11.12, “Integrated Windows domain logon” on page 460 for more information.

After completing this window and clicking **Next** -> **Advanced options** -> **Server connection**, the window shown in Figure 14-20 is displayed.



Advanced Options

Choose options to be configured

- HTML parameters
- Code base
- HTML templates
- Problem determination
- User updates
- Appearance
  - Applet size
- Other
  - Session Manager API
  - Server connection
  - Language
  - Maximum sessions

Server connection options

□ Use system defaults

If you are running Host On-Demand through a firewall, using the configuration servlet will eliminate the need to open an extra port for the configuration server.

Do you want to use the configuration servlet?

○ Yes

● No

Configuration Servlet URL:

Configuration Server Port: 8999

Figure 14-20 Server connection options

If **Use system defaults** is checked, the parameters in the config.properties file are used by the Host On-Demand applet.

During Host On-Demand installation, the config.properties file is created in the Host On-Demand publish directory except on z/OS servers. On z/OS servers, this file is named config.properties.ascii and must be created manually. The config.properties file is read by all Host On-Demand applets and provides a global way of setting HTML parameters. If the default connection port of 8999 was chosen during installation, this file would contain the parameter/value of:

```
ConfigServerPort=8999
```

If the Configuration Servlet is installed and a connection port is specified, the config.properties file will contain the following:

```
ConfigServletURL=hostname_or_IPaddress\HODConfig\hod
```

If you have changed the default settings, uncheck **Use system defaults** and enter your new values through the Deployment Wizard as shown in Figure 14-20. However, if you wish to use these setting for all your client's host sessions, we recommend that you update the config.properties file on your Host On-Demand server.

To override the Configuration Servlet values, select **Yes** and supply the URL to where the Configuration Servlet is installed. To override the Configuration Server port, select **No** to `Do you want to use the configuration servlet` and specify the new port.

Note that specifying a new Configuration Server Port value on this window does not change the port that the Configuration Server is "listening" on. It simply provides a ConfigServerPort parameter in this HTML file that overrides the ConfigServerPort specified in the config.properties file. Only end users of this HTML file will pick up this parameter. To change the Host On-Demand listening port, the administrator must modify the NSMprop file. See "Changing the Service Manager's configuration port" in the online help for details.

Returning to our scenario, we will assume that using the system defaults is sufficient. After completing the Additional Options window and clicking **Ok** -> **Next,** the File Output and Format window is displayed as shown in Figure 14-17 on page 536. Note that the Host Sessions window shown in Figure 14-6 on page 523 will not be shown since, with the Configuration Server-based model, the administrator uses the administration utility to define host sessions and their properties. The information is kept on the Configuration Server and not in the customized HTML files created by the Deployment Wizard.

After the files have been distributed to the Host On-Demand server, end users will access the HTML page in the same method as used by the HTML model. For example:

```
http://TheHODWebserver/hod/configmodel.html
```

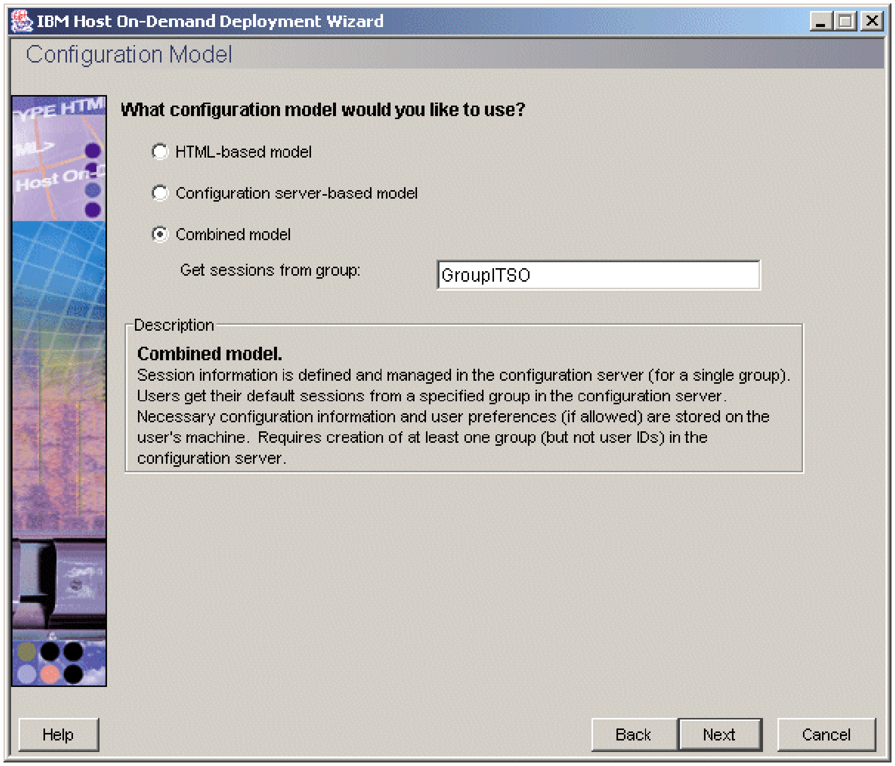
where configmodel is the name specified in the File Name field (see Figure 14-17 on page 536).

14.3.3 Combined model example

In the combined model host session, information is defined on the configuration server (like the configuration server-based model) and if allowed by the administrator, user preferences are stored on the user's machine (like the HTML-based mode). Unlike the configuration server-based model, Host On-Demand user IDs are not created on the configuration server. Configuration information is stored in group definitions on the server created through the administration utility. If the default session information within the group is ever changed by the administrator, the users of the HTML file will automatically receive the updates.

To illustrate the combined model in our scenario, we have chosen to use a Host On-Demand server installed on a z/OS platform. Since the Host On-Demand Configuration Server was installed on a z/OS system, the Deployment Wizard must be run on a Windows machine. In this example, the administrator will allow end users to save their user preferences.

After choosing to create a new HTML file, the window in Figure 14-21 is shown.



What configuration model would you like to use?

○ HTML-based model

○ Configuration server-based model

● Combined model

Get sessions from group: GroupITSO

Description

Combined model.
Session information is defined and managed in the configuration server (for a single group). Users get their default sessions from a specified group in the configuration server. Necessary configuration information and user preferences (if allowed) are stored on the user's machine. Requires creation of at least one group (but not user IDs) in the configuration server.

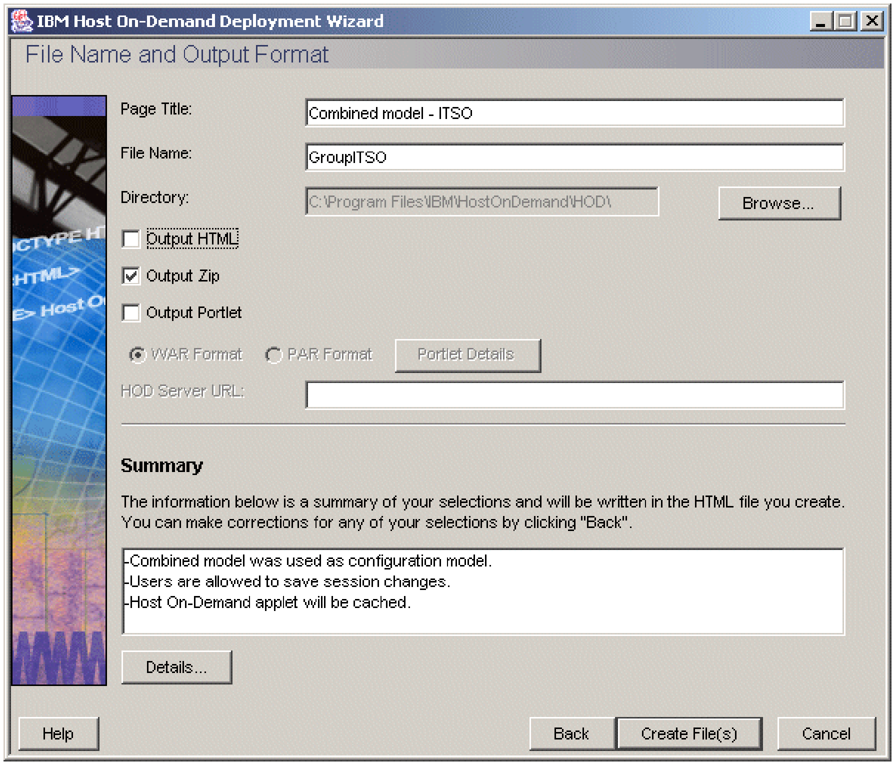
Figure 14-21 Combined model

The administrator selects the combined model and must also supply a group that is defined on the Configuration Server, GroupITSO. GroupITSO must be defined on the Host On-Demand server prior to end users accessing the customized HTML page because configuration information is obtained from this group. The administrator proceeds by clicking **Next** and the Additional Options window (shown in Figure 14-9 on page 526) is displayed.

Additional parameters can be selected in the same manner as the HTML and Configuration server-based model. Click **Next** to display the File Name and Output Format window. In this example the administrator selects **Output Zip** from the Output format window as shown in Figure 14-22. The file GroupITSO.zip will be stored in the default directory:

C:\Program Files\IBM\HostOnDemand\HOD

See 14.4, “Distributing Deployment Wizard files” on page 547 for information on deploying the custom HTML files.



File Name and Output Format

Page Title: Combined model - ITSO

File Name: GroupITSO

Directory: C:\Program Files\IBM\HostOnDemand\HOD\

□ Output HTML

☑ Output Zip

□ Output Portlet

● WAR Format ○ PAR Format

HOD Server URL:

Summary

The information below is a summary of your selections and will be written in the HTML file you create. You can make corrections for any of your selections by clicking "Back".

-Combined model was used as configuration model.
-Users are allowed to save session changes.
-Host On-Demand applet will be cached.

Figure 14-22 Output zip

Once the files are on the z/OS system, and the group containing the configuration information GroupITSO has been created by the administrator, end users can access these HTML files. For example:

```
http://TheHODWebserver/hod/GroupITSO.html
```

If the user makes any changes to the configuration information, these changes are stored on the user's local machine. As long as the applet is running, the Configuration Server on the z/OS host system should not be accessed again to obtain configuration information.

If the administrator makes a change to the configuration information in GroupITSO, the next time the user downloads the client, the new change will be picked up and merged with the user's preferences. For example:

1. The administrator initially sets up a 3270 session definition with a destination address of `sys1.raleigh.com` and a session name of `Raleigh System`.
2. The user downloads the applet and changes the session name to `My test system` (if this field is not locked).
3. Later, the system is moved and the destination address changes. The administrator logs on to the Administration Utility and changes the definition in GroupITSO to have a destination address of `sys2.raleigh.com`.
4. The next time the user downloads the applet, the new destination address will be used and saved, but the session name will remain since the user had previously specified, `My test system`. (This is true as long as the administrator did not also lock the session name field when the destination address was changed).

If the z/OS Web server is running, but the configuration server becomes unavailable, and the HTML files have been used at least once, the configuration settings on the user's local machine will be used to connect to the host system. A message is displayed to the end user and the Host On-Demand applet continues as usual.

If the HTML files have not been used, there is no locally stored preferences or session configuration information that can be used to launch a session; therefore, a message is displayed to the end user and the Host On-Demand applet stops running.

14.3.4 User preferences stored on local machines

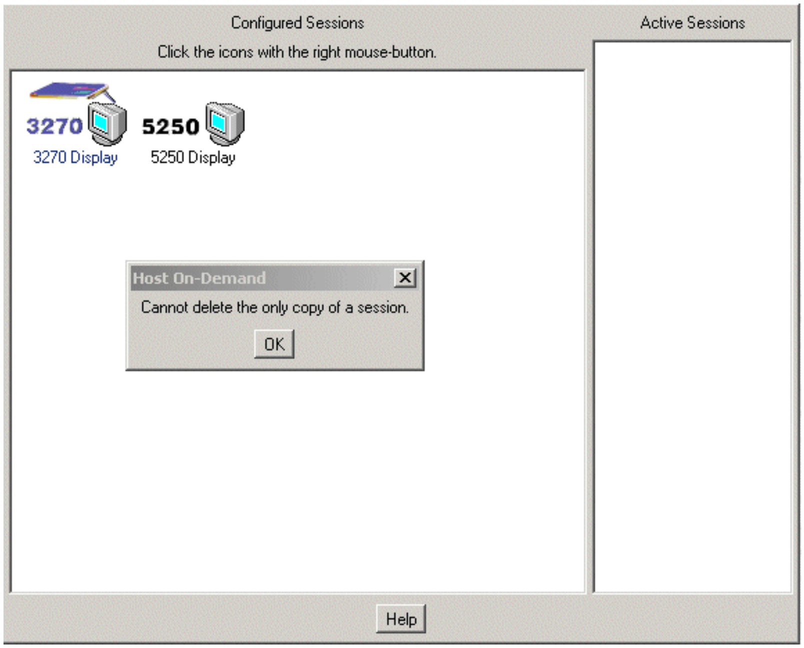
In the HTML-based model and combined model the default is to allow user changes to persist. User preferences are stored in files on the user's local machine. If the administrator has not allowed user changes to persist, there are no local files stored. There are some special considerations to be aware of when these models are used.

Browser considerations

Depending on which browser is used to access Host On-Demand, the files are stored in different locations. (See 14.5.3, "Files stored on local machine" on page 550 for more information.) This can cause confusion if an end user decides to use a different browser after making changes. The changes will not be picked up by the new browser. If as the administrator you are unable to restrict users to using a single browser, it is recommended to use the `Save` HTML parameter when creating the HTML files with the Deployment Wizard. (See Figure 14-15 on page 533.) This parameter allows the administrator to specify where the files are to be stored locally regardless of what browser the end user chooses.

Deleting sessions

An end user who has their user preferences stored on a local machine will not be allowed to delete the only copy of a session from the Host On-Demand Configured Sessions window. A message is displayed with this information. This is illustrated in Figure 14-23 where we tried to delete the session `3270 Display`.



Host On-Demand

Cannot delete the only copy of a session.

Figure 14-23   Deleting session error

Order of precedence for changes

When configuration information is kept in different places, there is an order of precedence as to which value is used when a change occurs in one place but not the other.

Initially, all values are created by the administrator. If the HTML-based model is used, the values are stored in the cfg*n*.cf file created by the Deployment Wizard. If the combined model is used, the values are stored in the Configuration Server. The initial download of the applet will use these values.

A user can change many of these values as long as the administrator has not locked the field. The user preferences are stored locally if the administrator has allowed changes to persist.

On subsequent downloads of the applet, configuration information is determined using the following hierarchy:

1. If a field is locked by the administrator, the value from the administrator is used.
2. If the user has made and kept changes locally, the values from the local user preferences are used.
3. If the administrator makes a change to a field that the user has not yet modified, or adds new configuration values, the values from the administrator are used.

> **Note:** Once a user has modified a field this value will override a subsequent change by the administrator. If as the administrator you wish to maintain control over certain fields it is recommended, use the lock function which will disable users from being able to make changes to the field.

Restoring the default preferences

To remove user changes and restore the default session properties, users can delete the files from their local machine that contains the user-specified changes. See 14.5.3, “Files stored on local machine” on page 550 to determine what files to delete. For example, to restore the defaults of a session called `3270 Payroll` that was set up in a customized HTML file called ITSO.html, look for a folder called ITSO on the local machine. If you delete this folder, all sessions defined in ITSO.html will be restored to their default settings. To restore a single session, open the folder **ITSO** and delete the cfgn.df file that contains the text string “`name=3270 Payroll`”.

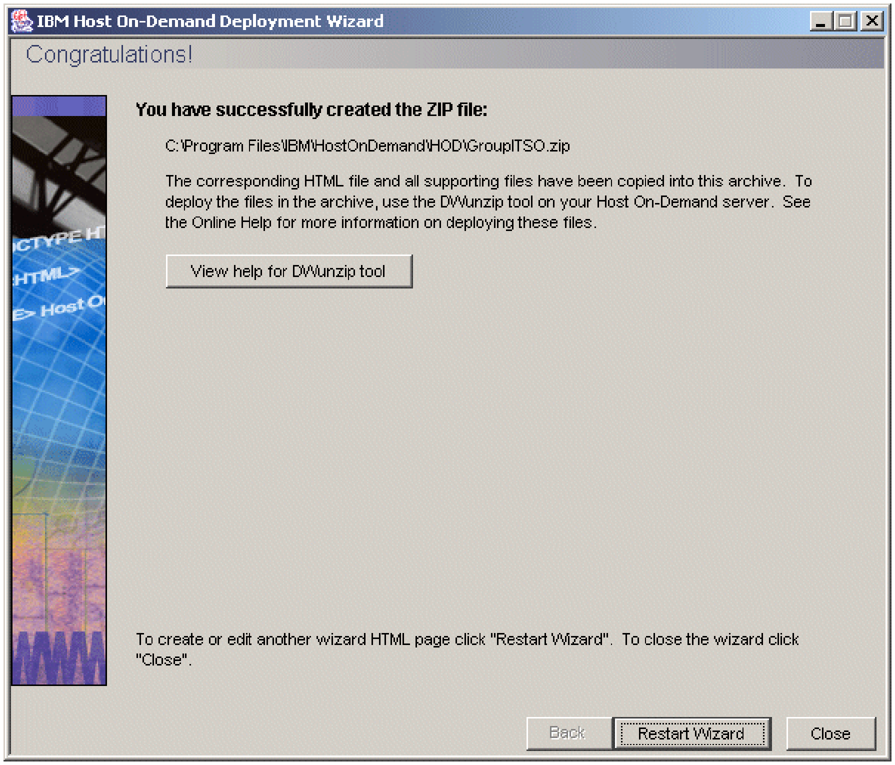
14.4 Distributing Deployment Wizard files

Once the custom HTML files have been created by the Deployment Wizard, they must be distributed to the production server. If Output Zip is checked the procedure is as follows:

1. Transfer the zip file created by the Deployment Wizard in binary to the server publish directory. This will either be the Host On-Demand publish directory or your user publish directory.
2. Edit the DWunzip file located on your server if necessary. You will need to edit the file if you have changed the default publish directory, or if you have transferred the zip file to your user publish directory.
3. If you are running DWunzip on a UNIX-based or z/OS platform, you will need to ensure DWunzip has execute permission.
4. Run DWunzip by entering `DWunzip xxxxx` where `xxxxx` is the name of the zip file created by the Deployment Wizard and transferred to the server.

> **Note:** Output Zip is recommended if your Host On-Demand server is on a different server or platform than your Deployment Wizard. The DWunzip tool ensures that files are stored in the appropriate directory. If your server is on a non-Windows platform, the DWunzip tool sets file permissions and ownership. If you are running DWunzip on a z/OS platform, the necessary file extensions are also added.

In the Combined Model example in Figure 14-22 on page 543 we entered `GroupITSO` in the File Name file and checked Output Zip. The output directory was not modified. After clicking **Create File(s)** the window in Figure 14-24 is displayed. This window displays the name of the zip file created and allows the administrator to view online help for using the DWunzip tool.


IBM Host On-Demand Deployment Wizard
Congratulations!
View help for DWunzip tool
Back
Restart Wizard
Close

You have successfully created the ZIP file:

C:\Program Files\IBM\HostOnDemand\HOD\GroupITSO.zip

The corresponding HTML file and all supporting files have been copied into this archive. To deploy the files in the archive, use the DWunzip tool on your Host On-Demand server. See the Online Help for more information on deploying these files.

To create or edit another wizard HTML page click "Restart Wizard". To close the wizard click "Close".

Figure 14-24 Dwunzip

If **Output HTML** is selected, the basic procedure is as follows:

1. Refer to 14.5, “Files created by the Deployment Wizard” on page 548 to help you determine the files that must transferred and the file format, either text or binary.
2. FTP the files to your configuration server platform.
3. If deploying the files to a UNIX platform, you will need to ensure file permissions are set correctly.
4. If the server is on a z/OS system, see Chapter 3.5, “Deployment Wizard considerations” on page 86 for special considerations.

14.5 Files created by the Deployment Wizard

There are several files that may be created by the Deployment Wizard. Not all files are created for every type of client, but the directory and file structure is identical for download and cached clients.

14.5.1 Files stored in publish directory

Table 14-1 lists the files that are created and must be stored in the server's Host On-Demand publish directory or your user publish directory. The default publish directory is:

```
\HostOnDemand\HOD
```

Table 14-1 Files stored in publish directory

File Name	Type	Description
xxxxx.html	text	HTML file created by Deployment Wizard; used by the end user to launch the client.
xxxxx_J2.html	text	HTML file created by the Deployment Wizard if Java 2 or Autodetect is selected.
z_*xxxxx*.html	text	HTML file created by the Deployment Wizard if Java 2 or Autodetect is selected.
where xxxxx is the File Name specified on the Output Format window of the Deployment Wizard. If Java 1 is selected xxxxx_J2.html and z_xxxxx.html will not be created.		

14.5.2 Files stored in customized subdirectory

For every customized HTML that is created, a corresponding subdirectory is created with the same name under \HODData. The default is:

```
\HostOnDemand\HOD\HODData\xxxxx
```

These files contain the session configuration information created by the administrator.

Table 14-2 lists the files created by the Deployment Wizard and stored in `\HODData\xxxxx`.

Table 14-2 Files stored in \HODData\xxxxx

File Name	Type	Description
cfg*n*.cf	text	One for each session defined; contains configuration information set by administrator.
params.txt	text	Contains some configuration parameters for the setup of the client session window.
policy.obj	binary	Contains information about the Disabled Functions; see Figure 14-8 on page 525.

File Name	Type	Description
preloads.obj	binary	Contains information about the objects to preload as defined on the Preload Options window; see Figure 14-16 on page 534.
udparams.txt	text	User-defined HTML parameters.
wInfo.txt	text	Contains the responses to each window in the Deployment Wizard; used only by the Deployment Wizard.
cfg*n*.cf and policy.obj will only be created if the HTML-based model is selected		

14.5.3 Files stored on local machine

If the HTML-based model or combined model is used in the Deployment Wizard and **Persist user changes** is checked, user preferences are kept on the local machine of the user.

Depending on which browser is being used to access Host On-Demand, the files that contain the user preferences can be in different directories. Table 14-3 lists the directories where local files will be stored.

Table 14-3 Default local directories

Platform and browser	Directory
Windows 98 & IE Windows 98 & Netscape 4 Windows 98 & Netscape 6	\Windows\Java\username\HODData\xxxxx \Netscape\Users\username\HODData\xxxxx \Windows\username\HODData\xxxxx
Windows 2000/XP & IE Windows 2000/XP & Netscape 4 Windows 2000/XP & Netscape 6	\Documents&Settings*username*\HODData\xxxxx \Netscape\Users\username\HODData\xxxxx \Documents&Settings\username\HODData\xxxxx
Windows NT & IE Windows NT & Netscape 4 Windows NT & Netscape 6	\WINNT\Profiles\username\HODData\xxxxx \Netscape\Users\username\HODData\xxxxx \WINNT\Profiles\username\HODData\xxxxx
OS/2 & Netscape 4 OS/2 & Netscape 6	\Netscape\Users\username\HODData\xxxxx \java13\JRE install dir\HODData\xxxxx
UNIX & Netscape 4 UNIX & Netscape 6	/home/username/.netscape/HODData/xxxxx /home/username/HODData/xxxxx

Where `xxxxx` is the name of the custom HTML file created, and username is the user ID of the logged-on user. With Netscape 4.x on Windows it represents the Netscape profile ID.

If the `Save` HTML parameter is specified when the HTML files is created, the files will be located in this directory, regardless of which browser is used:

```
<save base directory>\userID\HODData\xxxxx
```

Table 14-4 lists the files stored in this directory.

Table 14-4 Files stored on local machine

File Name	Type	Description
cfg*n*.cf	text	One for each session defined; contains configuration info set by administrator
cfg*n*.df	text	Difference file; contains config changes made by user; one for each session changed by user
metadata	text	Info needed for Host On-Demand processing
version	text	Info needed for Host On-Demand processing

14.6 Additional parameters

The following are some additional parameters that the administrator can specify in the window shown in Figure 14-15 on page 533. Do not use a text editor to manually add these parameters to the HTML file or they will be lost the next time the file is opened with the Deployment Wizard. Additional details on each parameter can be found in the online help for this window.

Table 14-5 Additional parameters

Parameter	Value	Description
3270InputAreaIndication	Underdot,DisplayAndNonDisplay UnderDot,NonDisplay UnderDot,Display UnderLine,Display UnderLine,DisplayAndNonDisplay UnderLine,NonDisplay 3DLowered,DisplayAndNonDisplay 3DLowered,Display 3DLowered,NonDisplay 3DRaised,DisplayAndNonDisplay 3DRaised,Display 3DRaised,NonDisplay	Indicates that the unprotected fields in a 3270 session be indicated in a particular method. Underdot - Causes a dot to be placed under every character position in the fields indicated by the second value. Underline - Causes an underline to be placed under every character position in the fields indicated by the second value. 3D - Causes a 3D rectangle to be displayed in the fields indicated by the second value. Display - Only unprotected displayable fields will have the selected indication applied. NonDisplay - Only unprotected nondisplayable fields will have the selected indication applied. DisplayAndNonDisplay - All unprotected fields will have the selected indication applied.
AdditionalArchives	Java 1 or Java 2 archives	Names of Java archives to be downloaded to the client workstation.
CustomKeyFunctionX	function identifier|function data	Customizes the list of functions that a key or key combination can be mapped to using keyboard remapping.
CustomTable	text file name	Specify character mapping tables to translate between PC and host code.
DebugCode	65535	Turns on debug tracing for the client. Enables debugging information to be written to the Java console. Java console must be enabled.
Disable	lum	Disables license use counting and License Use Management server reporting.
DisableSupport	true	Disables the support option of the Help menu.

Parameter	Value	Description
DoNotPrefillUser	true	Causes the logon window to come up with a blank userID field. If this parameter is absent, the default is to fill in the user ID with the user name requested from the system.
HideHODDesktop	true	Hides the Host On-Demand desktop and sessions tabs once an embedded sessions starts.Recommended only if one host session is configured which will be auto-started.
ForceJREInstall	true	Do not display popup when IBM Java 2 plug-in V1.4 is downloaded.
IgnoreWellKnownTrustedCAs	true	Prevent Host On-Demand from loading the WellKnownTrustedCAs.class file.
IPMonitor	SessionName= TraceFile=	Start IPMonitor utility automatically with session.
JVMMinimum	>=3165	Minimum Microsoft Java 1 level that Host On-Demand will require to run.
Save	base save directory	Specifies the location where the user preferences are to be stored. Only applies to Combined and HTML-based models.
ShareCachedClient	true	Enables Windows 2000 and XP multi-user machines (using IE and Microsoft JVM) to share an image of the cached client. See the online documentation for details regarding restricted users.
SharedCachedDirectory	fully qualified path	Specifies the directory location where the cached client will be installed.
SkipConfigProperties	true	Prevents reading of HTML parameters from the config.properties file.

15

Express Logon

This chapter describes the two Express Logon features offered with Host On-Demand V8:

- Web Express Logon (new in HOD V8)
- Certificate Express Logon (available since HOD V5)

Express Logon Feature (ELF) has been available since Host On-Demand V5, and is still available today. However, to better differentiate it from Web Express Logon, we now refer to ELF as Certificate Express Logon. Certificate Express Logon functions the same as ELF did in earlier versions, and requires the same configuration. Currently, Web Express Logon and Certificate Express Logon are the two types of Express Logon available with Host On-Demand V8. Although both Web Express Logon and Certificate Express Logon allow users to log on to host systems without having to enter their user IDs and passwords, the two types of Express Logon have different requirements.

Certificate Express Logon requires client-side certificates for user authentication, and works exclusively with 3270 session types. In order to use Certificate Express Logon, the client must have a valid client certificate, and the SSL connection must be made to one of the supported TN3270 servers.

Web Express Logon, however, does not require client-side certificates, and it can function with most Host On-Demand session types.

Which type of Express Logon you choose depends on your environment and your company needs.

Attention: Although Express Logon Feature (ELF) was renamed to Certificate Express Logon in Host On-Demand V8, current documentation outside of Host On-Demand still refers to it as *ELF*.

15.1 Web Express Logon

This section discusses the Web Express Logon feature introduced in Host On-Demand V8. Details on Certificate Express Logon can be found at 15.2, “Certificate Express Logon” on page 580.

15.1.1 Overview of Web Express Logon

The overall goal of Web Express Logon is to provide an automated way for users to log on to hosts and host-based applications without having to provide an additional user ID and password. It is designed to function within a wide range of computing environments. Your particular environment determines the way in which you plan for, implement, and use Web Express Logon.

Web Express Logon currently offers two styles of logon automation:

- Macro-based automation
- Connection-based automation

The style of logon automation that best suits your environment depends on your host and session type. If your host allows the client to supply the needed host credentials at the time the connection is established (for example, through a Kerberos passticket), connection-based automation is the appropriate style to use. However, if the client does not receive the needed credentials at the time the connection is established, and the host must send a login screen to authenticate the client, macro-based automation is the appropriate style. This style of automation requires a macro because the macro is responsible for automating the login screen. During this automation process, the macro populates the screen’s credential fields with the appropriate user information, and then transmits this information to the host for authentication.

The following sections provide more details about Web Express Logon’s macro-based and connection-based automation.

Macro-based automation

In order to use the macro-based automation style of Web Express Logon, you must have a network security application in place. Host On-Demand provides out-of-the-box support for three common network security applications without requiring additional coding:

- IBM Tivoli Access Manager
- Netegrity Siteminder
- Microsoft Active Directory (Windows Domain)

> **Important:** If you have a different network security application, you will need to create your own plug-in to work in your environment. For more information, refer to Customizing Web Express Logon in the Web Express Logon white paper at:
>
> `http://www.ibm.com/software/network/library/whitepapers/wel.pdf`

Macro-based automation relies on the following four key components and the interactions that take place among them:

- Credential Mapper Servlet (CMS)
- login macro
- Network Security plug-in
- Host Credential Mapper (HCM) database

The Credential Mapper Servlet is supplied with Host On-Demand and must be deployed to a Web server or some type of Web application framework. At a high level, the CMS is responsible for the following actions:

- Determine the client's identity (called a network ID)
- Map the user's network ID to the host ID
- Return the host credentials to the client as an XML document

The login macro automates the end-to-end process of the client sending the HTTPS request to the CMS, the CMS responding with the needed credentials, and the macro inserting the user's credentials in the proper fields to allow authenticated logon. You must record the login macro while you are in an active session. It initiates at the time the user attempts to access the host session, either automatically or manually (depending on your configuration).

Host On-Demand provides two Network Security plug-ins, one for IBM Tivoli Access Manager and one for Netegrity Siteminder. The Network Security plug-in does not apply to Microsoft Active Directory since the Windows login ID is used as the network ID. The primary function of the Network Security plug-in is to acquire the user's network ID, which may be gleaned from the HTTP header of the incoming HTTP request object.

The HCM database is a back-end repository that maps the users' network IDs to their host IDs. This repository can be a JDBC database such as one created with IBM DB2. The Digital Certificate Access Server (DCAS) and Vault plug-ins provided with Web Express Logon are designed to work with a such a database. Another possibility for a repository is an LDAP directory. However, using LDAP as your HCM database requires you to write your own HCM plug-in. For more information, refer to *Customizing Web Express Logon in the Web Express Logon* white paper at:

http://www.ibm.com/software/network/library/whitepapers/wel.pdf

Figure 15-1 illustrates the overall flow of macro-based automation by showing you the key components discussed above, and how they interact together to achieve logon automation.

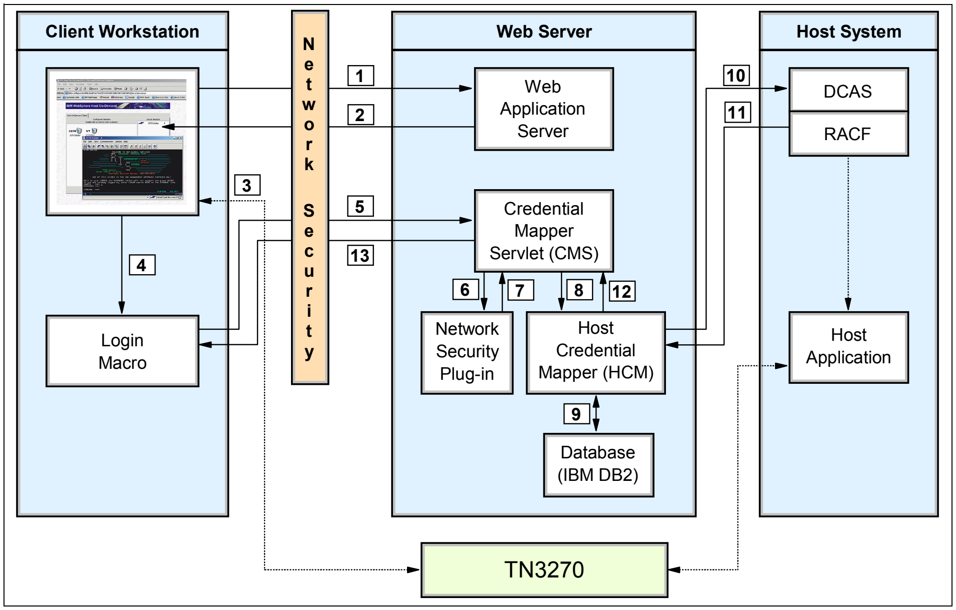


Figure 15-1 Macro-based automation in a z/OS and DCAS environment

The following are the steps that take place at the point when a user attempts to open a Host On-Demand session and initiates the login macro. If the macro is not configured to auto-start, the user will need to start it manually. The numbers in the list correspond to the numbers in Figure 15-1:

1. The end user clicks a link to the Host On-Demand desktop, which sends an HTTPS request through the network security application to the Web application server.

2. The Web application server returns the HTTPS request and the Host On-Demand desktop displays.
3. The user launches a host session.
4. The login macro executes.
5. The client sends an HTTPS request to the CMS to obtain the host credentials.
6. The CMS requests the user’s network ID from the Network Security plug-in.
7. The Network Security plug-in responds to the CMS with the user's network ID.
8. The CMS passes the network ID and application ID to the HCM plug-in.
9. Using the network and application ID, the HCM plug-in calls upon a database, such as IBM DB2, to map the user's host ID.
10. The HCM plug-in passes the user's host ID and application ID to the host and requests a password or passticket, depending on the type of HCM database. (In this example, The CMS sends the request to DCAS, a TCP/IP server application that interfaces with RACF, a Security Access Facility (SAF) compliant server product.)
11. The host (RACF) identifies the client, checks the client’s authorization, and returns the passticket to the HCM plug-in.
12. The HCM plug-in returns the host ID and passticket to the Credential Mapper Servlet.
13. The CMS returns the host credentials to the client as an XML document.

The login macro automatically inserts the user’s credentials in the logon screen fields without user intervention. Now the user is fully authenticated and can proceed with the session.

Macro-based automation has been successfully tested with (but is not limited to) the following applications:

- IBM Tivoli Access Manager for e-business Version 4.1
- Microsoft Active Directory
- Netegrity Siteminder Version 5.5
- WebSphere Application Server Versions 4 and 5
- IBM DB2 Universal Database™ Version 7 z/OS V1R4 with APAR PQ74457

Connection-based automation

Unlike macro-based automation, connection-based automation does not require a macro because the client and the host are able to connect without having to provide the user with a login screen. (In macro-based automation, a macro is required to automate this screen.)

Connection-based automation supports the following two environments:

- Telnet-negotiated login
- FTP login

Telnet-negotiated login

Currently, Web Express Logon supports OS/400 (V5R2 and later) Telnet-negotiated environments that have Kerberos authentication enabled. It does not require the CMS, a login macro, a Network Security plug-in, nor the HCM plug-in and database. Instead, it extends the existing single sign-on capability of the OS/400 operating system.

In order for connection-based automation to function in this environment, you must have the following prerequisites in place:

- Windows Domain Controller (Microsoft Active Directory)
- Key distribution center (KDC)
- Kerberos network authentication enabled on each target OS/400 system
- OS/400 V5R2 (5722-SS1) or later as the host operating system
- One or more of the following client operating systems:
  - Windows 2000 Professional and Server
  - Windows XP Professional
  - Windows server 2003

You must configure your OS/400 environment to use single sign-on capability in order to implement connection-based logon automation. The OS/400 environment provides single sign-on capability through a combination of network authentication service (NAS), and an IBM technology called Enterprise Identity Mapping (EIM). Host On-Demand uses this existing methodology for acquiring credentials to allow users to bypass the 5250 session login screen. Both NAS and EIM technology are available with the OS/400 (V5R2 and later) operating system.

Figure 15-2 illustrates the overall process of connection-based automation in an OS/400 environment with Kerberos authentication enabled.

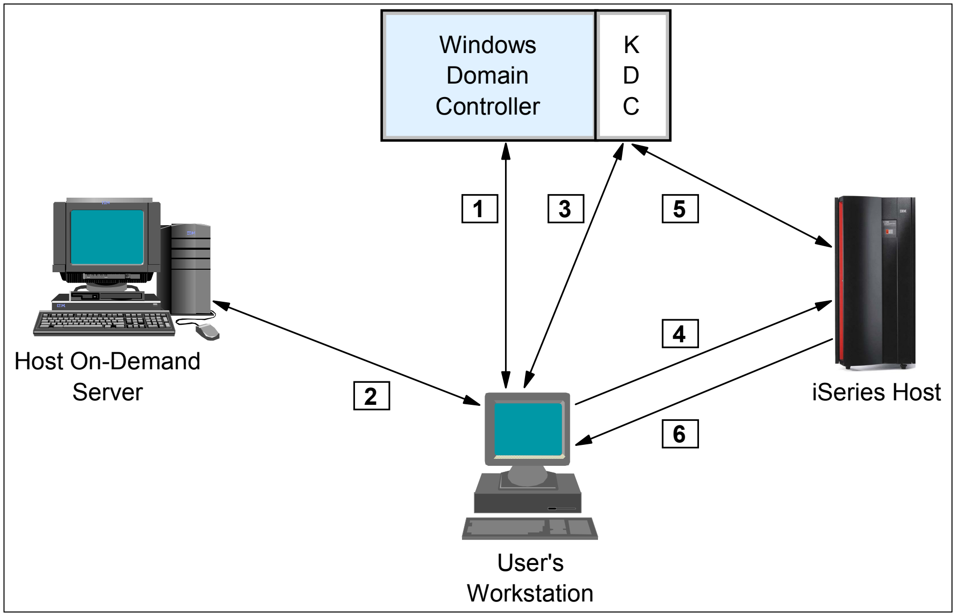


Figure 15-2 Connection-based automation in an OS/400 and Kerberos environment

Here are the steps:

1. A user logs on to the Windows domain. The Windows domain gives users access to the network.
2. The user requests a Host On-Demand session from the Host On-Demand server.
3. The Host On-Demand session initializes and requests a Kerberos ticket from the key distribution center. This is how users gain access to the individual resources within the network.
4. The user attempts to create a connection with the identified session using the Kerberos ticket as the credential.
5. The iSeries host validates the ticket with the KDC.
6. The user is successfully logged in.

FTP login

- Web Express Logon provides an automated way for users to log on to FTP hosts by providing a central repository for storing and retrieving user's credentials. Although this process is similar to configuring Web Express Logon in a vault-style environment, this type of automation is different because the user’s credentials are retrieved from the CMS at the time the connection is established. In other words, it does not require a macro. Currently, Host On-Demand allows you to statically store a user’s ID and password in the FTP configuration; however, Web Express Logon extends this approach by automating the user credential retrieval process.

For more specific information about enabling Web Express Logon for FTP sessions, look for the following icon throughout the remainder of this chapter:

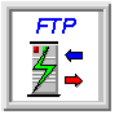


Figure 15-3 FTP icon

15.1.2 Implementing macro-based automation

Before you implement Web Express Logon with macro-based automation, you will need to take inventory of your environment and plan properly. Once you complete the following questionnaire, you should be ready to implement the Web Express Logon:

- What is your target host operating system? If your target host system is OS/400 V5R2 with Kerberos authentication enabled, connection-based automation is your preferred style of automation.
- Is your network security application one of the three applications that Web Express Logon supports (IBM Tivoli Access Manager, Netegrity Siteminder, Microsoft Active Directory)? If not, you will need to write your own Network Security plug-in. Since writing plug-ins requires J2EE knowledge and experience working with J2EE-compliant servlets, be sure you have someone on hand who has these skills.
- Do you need to configure your network security application to work with Web Express Logon? Recall that Web Express Logon’s Network Security plug-in must be able to acquire the user’s network ID in order to achieve logon automation.
- Do you have a J2EE-compliant Web application server to deploy the CMS to your Web server?
- What will you use as your HCM database? The DCAS and Vault plug-ins provided with Web Express Logon are designed to work with a JDBC database such as one created with IBM DB2. Another possibility is an LDAP directory. However, using LDAP as your HCM database requires you to write your own plug-in.

- Do you plan to use DCAS on a z/OS platform, or do you plan to use a vault-style database to acquire the host access credentials? The answer to this question will determine which parameters you add to the XML file when you are configuring the CMS. Also, if you are using DCAS to assist in the automation process, you will need to configure it to work with Web Express Logon as well as create an SSL key database file. For more information about configuring DCAS and creating an SSL key database file, refer to the Web Express Logon white paper at:

  `http://www.ibm.com/software/network/library/whitepapers/wel.pdf`

Once you have answered these questions, you are ready to start implementing Web Express Logon. Perform the following steps:

1. Create the Host Credential Mapper database.

   The HCM database is one of the key players in the Web Express Logon process because it maps the users' network IDs to their host IDs. Without this mapping, single sign-on capability is lost because users still need to log on to their host sessions manually.

   The DCAS and Vault parameters supplied with Web Express Logon are designed to work with a JDBC database such as one created with IBM DB2. Using this type of network-accessible database provides a flexible means of associating users' network IDs with their host IDs. If you are using a different type of repository, such as LDAP, you will need to create your own HCM plug-in. For more information, see *Customizing Web Express Logon* in the Web Express Logon white paper for more information:

   `http://www.ibm.com/software/network/library/whitepapers/wel.pdf`

   If you are using DCAS to assist in the automation process, create a table with the following column headings (in all uppercase). These columns will correspond to the DCAS parameters that you will add to the servlet configuration file (web.xml) in the next step:

   – NETWORKID: This column contains the network IDs of the users. A user's network ID is the credential that uniquely identifies the user to the network security application (in this case, Tivoli Access Manager).

   – HOSTADDRESS: The column contains the destination host address. This address can either be the host's IP address or the fully qualified URL, for example, amin.raleigh.ibm.com.

   - APPLICATIONID: This column contains the application IDs of the users. Application IDs are used to map users' host IDs and to retrieve passtickets from the RACF server.

     The APPLICATIONID column is not required for FTP sessions.

   - HOSTID: This column contains the users’ host IDs. A host ID is the credential used to uniquely identify the user to the host being accessed.

     If you are using a vault-style database to acquire the host access credentials, you will need to add these same four column headings to your HCM database, plus this additional one below.

   - PASSWORD: This column contains the users’ host passwords. Similar to a DCAS passticket, this password is used to map the users' network IDs to the host IDs; however, it requires an additional parameter in the servlet configuration file, which you will edit in the next step.

2. Configure the Credential Mapper Servlet.

   The CMS is the core of the credential-mapping framework. At a high level, the CMS is responsible for the following tasks: (1) Determine the client's identity (called a network ID), (2) Map the user's network ID to the host ID, and (3) Return the host credentials to the client as an XML document.

   Host On-Demand provides three CMS WAR files, one for each of the following network security applications:

   - IBM Tivoli Access Manager for e-business V4.1
   - Netegrity Siteminder V5.5
   - Microsoft Active Directory (Windows Domain)

   If you have a different network security application, you will need to customize your own version of the CMS. For more information about how to do this, refer to *Customizing Web Express Logon* in the Web Express Logon white paper at:

   http://www.ibm.com/software/network/library/whitepapers/wel.pdf

   In addition to several CLASS files, the WAR files contains the following four files:

   - web.xml
   - DCAS.xml
   - Vault.xml
   - was.policy

The web.xml file is the servlet configuration file that you will edit using some type of Web application server application, such as IBM WebSphere Application Server. The other two XML files (DCAS.xml and Vault.xml) are sample files that are included to help you better understand DCAS and Vault parameters and their values. We recommend that you use these files as a reference when you edit the web.xml file. Finally, the was.policy file is for IBM WebSphere Application Server only. It contains the required permissions for the CMS when Java 2 security is enabled. For more information about this, refer to *Troubleshooting Web Express Logon* in the Web Express Logon white paper at:

`http://www.ibm.com/software/network/library/whitepapers/wel.pdf`

To configure the CMS, perform the following steps:

a. Locate the WAR files on the Host On-Demand CD.

   Browse to the apps\wel directory to locate the three WAR files supplied with Host On-Demand. Table 15-1 shows which files correspond to which network security application.

Table 15-1 Web Express Logon WAR files

Network security application	Corresponding WAR file
IBM Tivoli Access Manager for e-business V4.1	amcms.war
Netegrity Siteminder V5.5	smcms.war
Microsoft Active Directory (Windows Domain Controller)	wincms.war

b. Edit the CMS-related INIT parameters.

> **Tip:** Refer to DCAS.xml and Vault.xml, located in the WAR file, to see examples of what your web.xml file should contain once you finish editing it.

- In the web.xml file, locate the CMPICredentialMappers parameter and change its value from echo to the name of your HCM plug-in; for example, CMPIDCASPlugin if you are using DCAS, or CMPIVaultPlugin if you are using a vault-style database to acquire the host access credentials.

FTP

For FTP sessions, the name of your HCM plug-in is CMPIVaultPlugin.

- Replace the echo parameter name with the value that you entered for the CMPICredentialMappers parameter (CMPIDCASPlugin or CMPIVaultPlugin). Change the parameter value to the full class path name of the implementing class, the authentication type to be used by the HCM, and the host mask.

  Full class path name: The CMS uses the value of the full class path name to create a class object of the specified type. That object is then used to handle CMS or HCM plug-in requests. The specified class file must be in the ...\WEB-INF\classes subdirectory in a loose file (not as a JAR file). From this location, the CMS will be able to access and use it whenever the need arises.

  Authentication type: This parameter value is used to identify the type of authentication that the requestor needs. Once you specify the desired authentication type, the CMS can better identify which HCM plug-in to select to handle the request. You can pair multiple authentication types together to give HCM plug-ins the freedom to support multiple authentication types. Use the vertical bar character to join multiple authentication types. The five identified authentication types and descriptions are listed in Table 15-2.

Table 15-2 Authentication types and descriptions

Authentication type	Description
AuthType_3270Host	Identifies the credentials to be used with a 3270 emulation
AuthType_5250Host	Identifies the credentials to be used with 5250 emulation
AuthType_VTHost	Identifies the credentials to be used with VT emulation
AuthType_FTPPassword	Credentials used to access an FTP host
AuthType_ConfigServer	Credentials identified by the token used to identify the user to the Host On-Demand configuration server (if you are using the Configuration server-based model
AuthType_All	This type identifies the credentials to be used with all authentication types.

Host mask: The host mask is a secondary selection criteria used by the CMS to identify the most appropriate HCM plug-in. This value can contain one or more host addresses. Use the vertical bar character to join multiple addresses. Use the asterisks character to wildcard a host address. The wildcard character may start, end, or start and end a host address. Table 15-3 lists valid wild-carded addresses.

Table 15-3 Host mask and value matched

Host mask	Value matched
*.raleigh.ibm.com	Matches all addresses that end with .raleigh.ibm.com
ralvm*	Matches all addresses that start with ralvm
*	Matches all
xyz	Matches any host address that contains xyz

c. Add the optional CMS-related debugging parameters.

Add the following two optional debugging parameters to help you troubleshoot:

CMPI_TRACE_LOG_FILE
This parameter specifies the name of the log file. The value should be the full path to the log file, for example:

```
C:\Program Files\IBM\HostOnDemand\HODWEL.log
```

on a Windows platform.

CMPI_CMS_TRACE_LEVEL
This parameter specifies the trace level for the CMS. The trace messages are logged to the log file specified by CMPI_TRACE_LOG_FILE parameter. Depending on your Web application server, they may or may not be logged to the console. Trace level values include the following:

- 0 = None: No tracing. This is the default.
- 1 = Minimum: Trace APIs and parameters, return values, and errors.
- 2 = Normal: Trace Minimum plus internal APIs and parameters and informational messages.
- 3 = Maximum: Trace Normal plus Java exceptions.

d. Add the required parameters for CMPIDCASPlugin or CMPIVaultPlugin.

If you are using DCAS on a z/OS host, you must add the required DCAS plug-in parameters; and if you are using a vault-style database to acquire the host access credentials, you must add the required Vault plug-in parameters. Adding these parameters allows the HCM database to map the users' network IDs to their host IDs, and then retrieve a passticket (DCAS) or password (Vault) from the host.

FTP sessions require Vault parameters, not DCAS parameters.

Required DCAS parameters

The following two Host Credential plug-in parameters allow the client to connect to the DCAS server securely:

CMPI_DCAS_KEYRING_FILE
This parameter references the SSL keyring database file that you created either using the Host On-Demand Certificate Management tool or the P12 keyring tool. This file provides access to the DCAS client certificate as well as the DCAS server's certificate. The certificates establish a client-authenticated secure connection with the DCAS server. The DCAS plug-in serves as the DCAS client.

CMPI_DCAS_KEYRING_PASSWORD
This parameter specifies the password for the keyring database.

> **Important:** We strongly recommend that you encrypt this parameter using the password encryption tool provided with Host On-Demand. The tool encrypts the password and then decrypts it so the HCM can use it. To learn more about how to use this tool, refer to Appendix D, "Web Express Logon" on page 1063.

The following parameters contain all the relevant information needed to connect to your HCM database. You can either configure access to an existing database or to a newly created one. The level of security for the database depends on the database vendor.

If you are using an LDAP directory as your HCM database, you will need to create your own HCM plug-in. For more information, refer to *Customizing Web Express Logon* in the Web Express Logon white paper at:

`http://www.ibm.com/software/network/library/whitepapers/wel.pdf`

CMPI_DCAS_DB_ADDRESS
This is a URL string that provides the address of the database. An example of this string is jdbc:db2://dtagw:6789/CMTEST.

CMPI_DCAS_DB_NET_DRIVER
This string contains the name of the class that acts as the network database driver. An example of this string is `COM.ibm.db2.jdbc.net.DB2Driver`. The location of this class is assumed to be in the existing class path.

CMPI_DCAS_DB_USERID
This is the ID of the user account to use when accessing the database.

CMPI_DCAS_DB_PASSWORD
This is the password of the user account to use when accessing the database.

Important: We strongly recommend that you encrypt this parameter using the password encryption tool provided with Host On-Demand. The tool encrypts the password and then decrypts it, so the HCM can use it. To learn more about how to use this tool, refer to Appendix D, "Web Express Logon" on page 1063.

CMPI_DCAS_DB_TABLE
This entry identifies the table to use for the needed query.

The following four parameter values should match the column names in your HCM database and should clearly indicate the contents of the columns. With some databases, such as IBM DB2, the four column headings in the database must be in all uppercase, for example, NETWORKID, HOSTADDRESS, APPLICATIONID, and HOSTID.

CMPI_DCAS_DB_NETID_COL_NAME
This entry identifies the name of the column that contains the network ID value (NETWORKID).

CMPI_DCAS_DB_HOSTADDR_COL_NAME
This entry identifies the name of the column that contains the host address value (HOSTADDRESS).

CMPI_DCAS_DB_HOSTAPP_COL_NAME
This entry identifies the name of the column that contains the host application value (APPLICATIONID).

CMPI_DCAS_DB_HOSTID_COL_NAME
This entry identifies the name of the column that contains the user's host identification value (HOSTID).

Based on the information provided by the parameters above, you can make an SQL query of the database to get the host ID. This query uses the network ID, the host address, and the host application as keys for the query. The result is identified in the Host Identification column. Assuming that the query is successful, a call is made to the DCAS server to request the passticket.

Required Vault parameters

CMPI_VAULT_DB_ADDRESS
This is a URL string that provides the address of the database. An example of this string is jdbc:db2://dtagw.raleigh.ibm.com:6789/HODSSO.

CMPI_VAULT_DB_NET_DRIVER
This string contains the name of the class that acts as the network database driver. An example of this string is COM.ibm.db2.jdbc.net.DB2Driver. The location of this class is assumed to be in the existing class path.

CMPI_VAULT_DB_USERID
This is the ID of the user account to use when accessing the database. In this case, the user ID is admin.

CMPI_VAULT_DB_PASSWORD
This is the password of the user account to use when accessing the database.

> **Important:** We strongly recommend that you encrypt this parameter using the password encryption tool provided with Host On-Demand. The tool encrypts the password and then decrypts it so the HCM can use it. To learn more about how to use this tool, refer to Appendix A: Using the Password Encryption Tool.

CMPI_VAULT_DB_TABLE
This identifies the table to use for the needed query. In this case, the table is called HACP.

The following parameters should match the column names in your HCM database, and should clearly indicate the contents of the columns. With some databases, such as IBM DB2, the five column headings in the database must be in all uppercase, for example: NETWORKID, HOSTADDRESS, APPLICATIONID, HOSTID, and PASSWORD.

The APPLICATIONID column is not required for FTP sessions.

Based on the information provided by the first three of these parameters (network ID, host address, and the host application ID), you can make a SQL query of the database to get the host ID. The result of the query is entered in the host ID (HOSTID) column. Assuming that the query is successful, a call is made to the vault-style database to request the password.

CMPI_VAULT_DB_NETID_COL_NAME
This entry identifies the name of the column that contains the network ID value (NETWORKID).

VAULT_DB_HOSTADDR_COL_NAME
This entry identifies the name of the column that contains the host address value (HOSTADDRESS).

CMPI_VAULT_DB_HOSTAPP_COL_NAME
This entry identifies the name of the column that contains the host application value (APPLICATIONID).

VAULT_DB_HOSTID_COL_NAME
This entry identifies the name of the column that contains the host ID value (HOSTID).

CMPI_VAULT_DB_HOSTPW_COL_NAME
This entry identifies the name of the column that contains the host password value (PASSWORD).

e. Add the optional DCAS and Vault parameters (if desired).

Unlike the previous set of DCAS and Vault parameters, the following parameters are optional. Which of these parameters you add to the web.xml file depends on your environment and your objectives as an administrator:

Optional DCAS parameters

CMPI_DCAS_TRACE_LEVEL
This parameter specifies the trace level for the DCAS plug-in. The trace messages are logged to the log file specified by CMPI_TRACE_LOG_FILE parameter. Depending on your Web application server, they may or may not be logged to the console. Trace level values include the following:

- 0 = None: No tracing. This is the default.
- 1 = Minimum: Trace APIs and parameters, return values, and errors.
- 2 = Normal: Trace Minimum plus internal APIs and parameters and informational messages.
- 3 = Maximum: Trace Normal plus Java exceptions.

CMPI_DCAS_HOST_PORT
The DCAS host address is determined based on the destination host specified in the request. The default port address of 8990 is used, but you may override it using this parameter.

CMPI_DCAS_USE_WELLKNOWN_KEYS
This parameter indicates whether the WellKnownTrustedCAs.class should be used to look up the DCAS server certificate or not. The WellKnownTrustedCAs.class file must be in the root directory of the CMS. The default is true.

CMPI_DCAS_VERIFY_SERVER_NAME
This parameter indicates if the server host name in the certificate must be verified in addition to the certificate validation. The default is false.

CMPI_DCAS_REQUEST_TIMEOUT
This parameter specifies the passticket request timeout in milliseconds. It should be less than the Host On-Demand macro time-out value. The default is 50000.

CMPI_DCAS_DB_PRESERVE_WHITESPACE
This parameter indicates whether to trim white spaces from the credential request parameters or not. If true, the white spaces are not trimmed. The default is false.

Optional Vault parameters

CMPI_VAULT_TRACE_LEVEL
This parameter specifies the trace level for the Vault plug-in. The trace messages are logged to the log file specified by CMPI_TRACE_LOG_FILE parameter. Depending on your Web application server, they may or may not be logged to the console. Trace level values include the following:

- 0 = None: No tracing. This is the default.
- 1 = Minimum: Trace APIs and parameters, return values, and errors.
- 2 = Normal: Trace Minimum plus internal APIs and parameters and informational messages.
- 3 = Maximum: Trace Normal plus Java exceptions.

CMPI_VAULT_DB_PRESERVE_WHITESPACE
This parameter indicates whether to trim white spaces from the credential request parameters or not. If true, the white spaces are not trimmed. The default is false.

3. Repackage and deploy the WAR file.

   Once you finish configuring the CMS, repackage the WAR file and deploy it to your Web server. Refer to your Web server application's documentation for details of how to repackage and deploy the servlet.

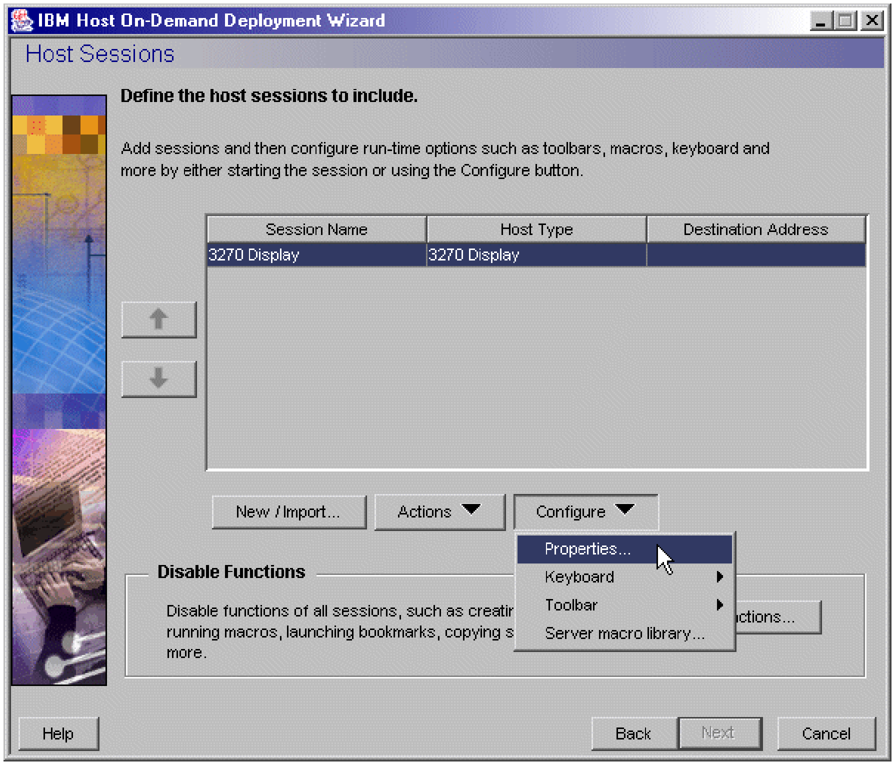
4. Enable Web Express Logon with the Host On-Demand Deployment Wizard.

   In order to enable Web Express Logon, you must create your HTML file, configure your HTML session, and record the login macro. You can do all three of these tasks within the Deployment Wizard:

   a. To create your HTML file, follow the instructions in the Chapter 14, “Deployment Wizard” on page 517.

   b. To configure your HTML session for Web Express Logon within the Deployment Wizard, navigate to the Host Sessions window (Figure 15-3), highlight your 3270 Display session, and click **Configure -> Properties.**

      IIf you are configuring an FTP session, your Session Name will be FTP, and your Host Type will be FTP/sftp.



Host Sessions

Define the host sessions to include.

Add sessions and then configure run-time options such as toolbars, macros, keyboard and more by either starting the session or using the Configure button.

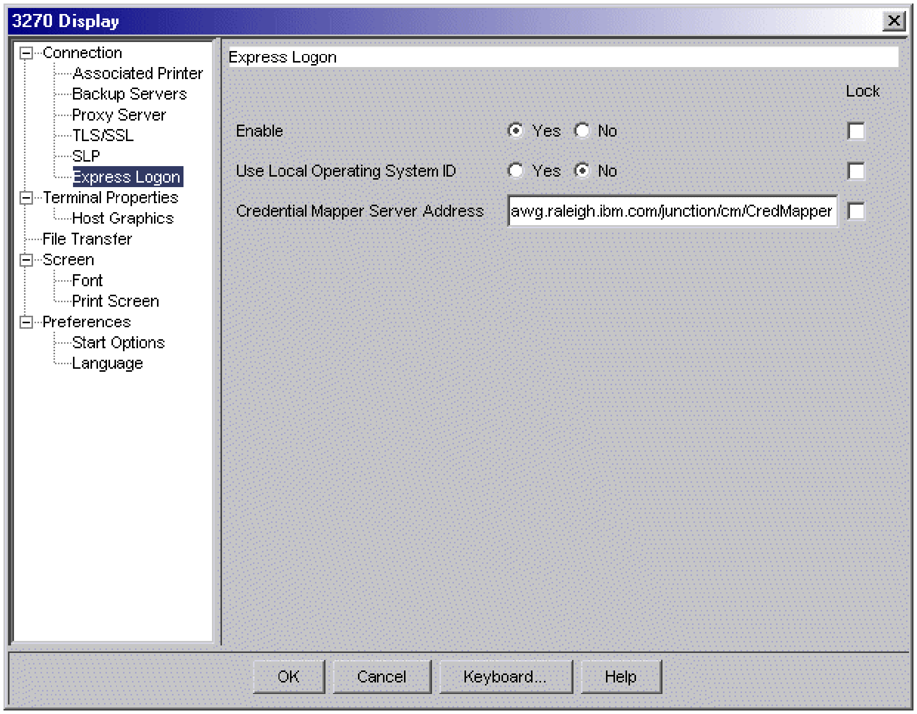
Session Name	Host Type	Destination Address
3270 Display	3270 Display	

Disable Functions

Disable functions of all sessions, such as creatir running macros, launching bookmarks, copying s more.

Figure 15-4 Configuring 3270 Display session properties within the Host Sessions

Under the Connection option on the left side of the 3270 Display window (Figure 15-5), click **Express Logon**. Select **Yes** to enable Express Logon and chose whether or not you want Host On-Demand to use the user's local operating system ID for authentication.



Express Logon

		Lock
Enable	● Yes ○ No	□
Use Local Operating System ID	○ Yes ● No	□
Credential Mapper Server Address	awg.raleigh.ibm.com/junction/cm/CredMapper	□

Figure 15-5 3270 Display window

Next, type the full URL of the credential mapper server, for example, `https://server_name/junction/cm/CredMapper`, where:

- server_name is the name of the authentication server
- junction is the name of the junction point (optional)
- cm is the credential mapper servlet space
- CredMapper is the servlet name

Click **OK**.

Be sure that the servlet name matches the name in your XML file. For example, if you specify the servlet name in your host session as CredMapper (recommended), the code in your XML should look like the following:

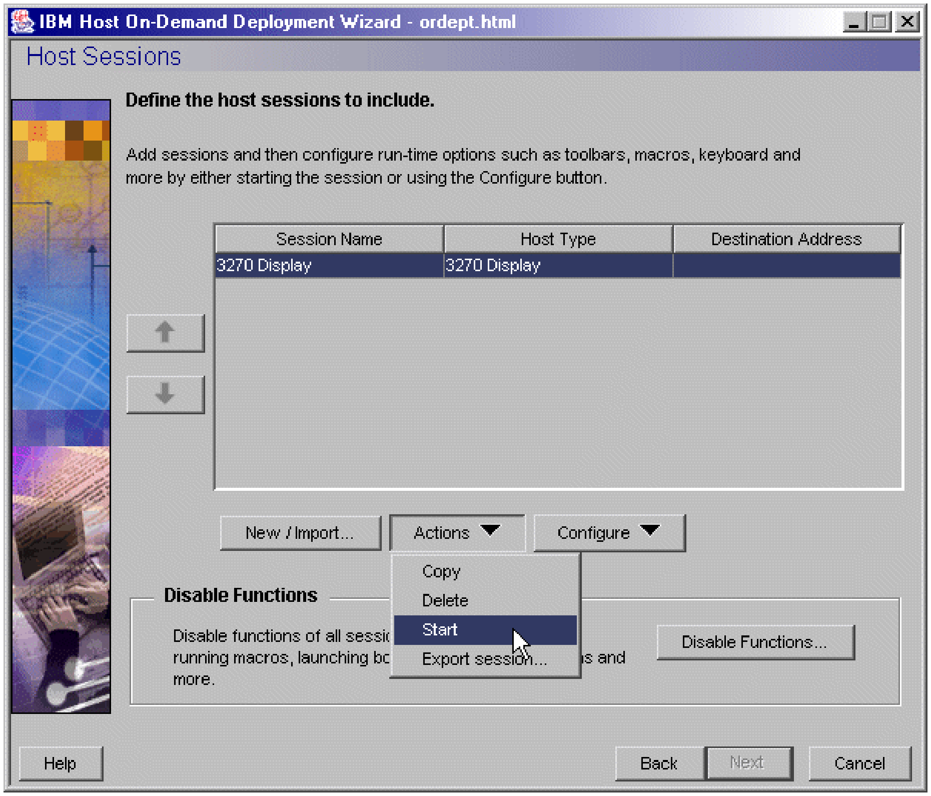
```
<servlet>
<servlet-name>CredMapper</servlet-name>
<display-name>CredMapper</display-name>
<servlet-class>com.ibm.eNetwork.security.sso.cms.CredMapper</serv
let-class>
```

The servlet that resides at this URL processes the HTTPS request from the user, performs a lookup, and returns the user's credentials. The Host On-Demand client uses the obtained credentials to automate the login process.

When configuring properties for FTP sessions, there is a Logon option in the left panel of the window. On this panel, be sure that you leave the User ID and Password fields blank if you are enabling Web Express Logon. If you add a user ID and/or password, Host On-Demand will ignore the settings on the Express Logon panel.

c. To record your login macro within the Deployment Wizard, navigate to the Host Sessions window (Figure 15-6), highlight your session, and click **Actions -> Start.** To record the login macro, you must be in an active session.

A login macro is not required for FTP sessions.



IBM Host On-Demand Deployment Wizard - ordept.html

Host Sessions

Define the host sessions to include.

Add sessions and then configure run-time options such as toolbars, macros, keyboard and more by either starting the session or using the Configure button.

Session Name	Host Type	Destination Address
3270 Display	3270 Display	

Disable Functions

Disable functions of all sessic running macros, launching bc ıs and more.

Figure 15-6 Starting a session within the Host Sessions window

For complete, step-by-step instructions of how to record your login macro and troubleshoot Web Express Logon, refer to the Web Express Logon white paper at:

`http://www.ibm.com/software/network/library/whitepapers/wel.pdf`

15.1.3 Implementing connection-based automation

Before you implement Web Express Logon with connection-based automation, you will need to take inventory of your environment and plan properly. Once you complete the following questionnaire, you should be ready to implement Web Express Logon:

- What level of OS/400 are you running on your iSeries host or hosts? It must be V5R2 (5722-SS1) or later in order to use connection-based automation.
- Are all the PCs in your network configured in a Windows 2000 domain? If not, configure them.

- Is iSeries Access for Windows (5722-XE1) installed on the PC that you will use to configure NAS?
- Do you have one of the following installed on the secure system that will act as the KDC? If so, which one?
  - Windows 2000 or Windows 2003 Server
  - AIX Server
  - zSeries
- Have you applied the latest program directory fixes (PTFs)? The latest PTFs are located on the iSeries support site at:

  `http://www.ibm.com/servers/eserver/support/iseries`.

For a more complete list of prerequisites and pre-configuration issues, refer to “Scenario #3: Connection-based automation” in the Web Express Logon white paper at:

`http://www.ibm.com/software/network/library/whitepapers/wel.pdf`.

Once you have answered these questions, you are ready to start implementing Web Express Logon. Perform the following steps:

1. Enable OS/400 single sign-on.

   Enabling single sign-on capability in an OS/400 V5R2 or later environment requires two types of configuration: network authentication service (NAS) and Enterprise Identity Mapping (EIM), both of can be configured using the iSeries Navigator tool in the IBM iSeries Access for Windows product. For detailed information, refer to the Web Express Logon white paper at:

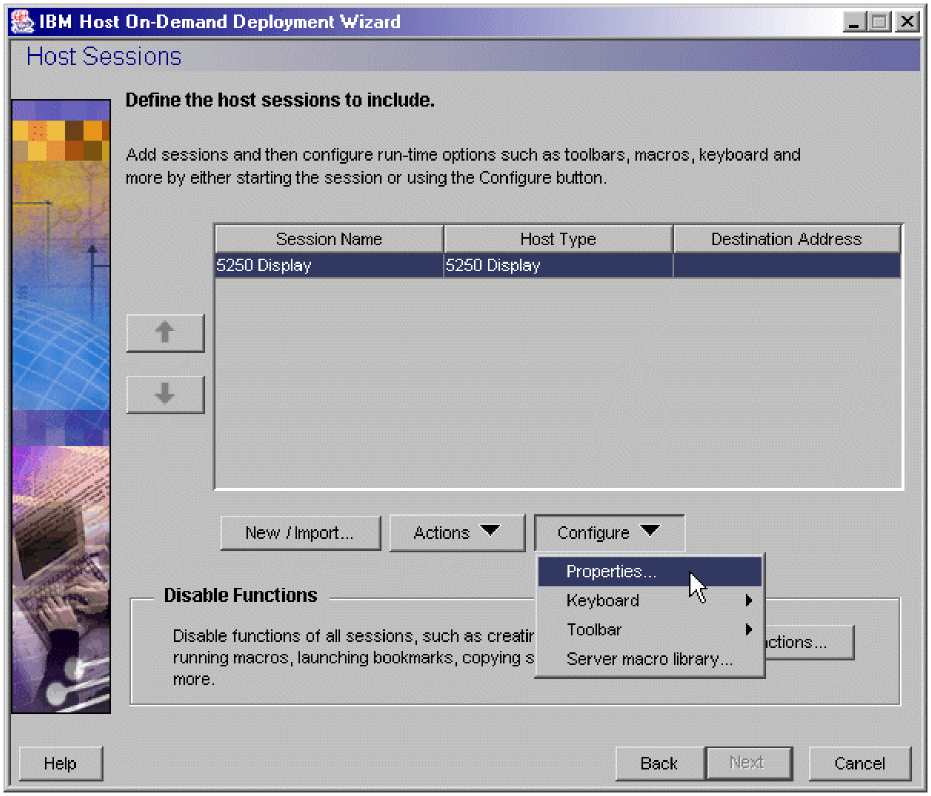
   `http://www.ibm.com/software/network/library/whitepapers/wel.pdf`.

2. Enable Web Express Logon with the Host On-Demand Deployment Wizard.

   In order to enable Web Express Logon, you must create your HTML file, configure your HTML session, and record the login macro. You can do all three of these tasks within the Deployment Wizard:

   a. To create your HTML file, follow the instructions in the Chapter 14, “Deployment Wizard” on page 517.

   b. To configure your HTML session for Web Express Logon within the Deployment Wizard, navigate to the Host Sessions window (Figure 15-7), highlight your 5250 Display session, and click **Configure -> Properties.**



Define the host sessions to include.

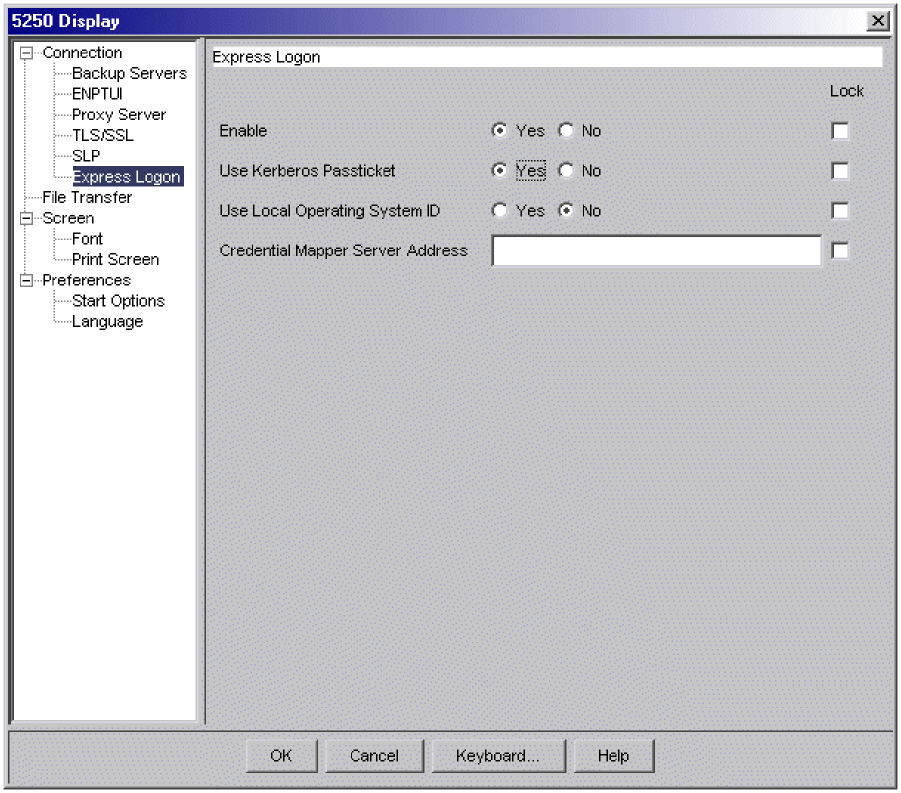
Add sessions and then configure run-time options such as toolbars, macros, keyboard and more by either starting the session or using the Configure button.

Session Name	Host Type	Destination Address
5250 Display	5250 Display	

Disable functions of all sessions, such as creatir running macros, launching bookmarks, copying s more.

Figure 15-7 Configuring 5250 Display session properties within the Host Sessions

Under the Connection option on the left side of the 5250 Display window (Figure 15-8), click **Express Logon**. Select **Yes** to enable Express Logon, and **Yes** to Use Kerberos Passticket.



Express Logon

Lock

Enable ● Yes ○ No □

Use Kerberos Passticket ● Yes ○ No □

Use Local Operating System ID ○ Yes ● No □

Credential Mapper Server Address □

Figure 15-8 5250 Display window

Once you select to use a Kerberos Passticket, Host On-Demand will be able to retrieve a passticket from a Windows server. This passticket is used to connect to the host system that you identify in the session properties.

Accept the default **No** for Use Local Operating System ID, and leave the Credential Mapper Server Address field blank. You only need to set these options if you have additional credential challenges that you want to automate through a vault-style setup. They do not apply to Kerberos authentication.

Click **OK** to return to the Host Sessions window.

For instructions of how to finish creating your HTML file, refer to the instructions in Chapter 14, "Deployment Wizard" on page 517.

To troubleshoot Web Express Logon, refer to the Web Express Logon white paper at:

http://www.ibm.com/software/network/library/whitepapers/wel.pdf.

15.2 Certificate Express Logon

This section discusses the Certificate Express Logon feature introduced in Host On-Demand V5. Details on Web Express Logon can be found at 15.1, “Web Express Logon” on page 556.

In previous releases of Host On-Demand and z/OS, Certificate Express Logon was known as the Express Logon Feature (ELF). In Host On-Demand V8, the Express Logon Feature was renamed to Certificate Express Logon.

For more information about Certificate Express Logon, refer to the *Setting up and Using the IBM Express Logon Feature* white paper on the Host On-Demand library page:

http://www.ibm.com/software/webservers/hostondemand/library.html

15.2.1 Overview and design of Certificate Express Logon

Certificate Express Logon allows a user running a 3270 client session to log on to a host system without entering a user ID and password. Certificate Express Logon is invoked through a macro that uses digital certificates in place of user IDs and passwords to log the user on to RACF-enabled applications. Using Certificate Express Logon reduces the number of user IDs and passwords that users need to remember.

Certificate Express Logon is supported on two-tier and three-tier network designs. The two-tier design utilizes the z/OS TN3270 Telnet server. The three-tier design utilizes a middle-tier TN3270 server and a Digital Certificate Access Server (DCAS).

In order for an application to be accessed using the Certificate Express Logon, a PassTicket data class profile (PTKTDATA) must be defined on each target RACF-enabled system (that is, the host where DCAS is running, and any host where RACF and a target application is located).

Both network designs require a TN3270 client workstation that supports Secure Sockets Layer (SSL) connections with client authentication and an X.509 certificate. Using RACF services in z/OS, the client certificate must be associated with a valid user ID. The only client-side product that supports the Certificate Express Logon is IBM WebSphere Host On-Demand V5 and later.

Two-tier network design

In the two-tier design, the user starts an SSL connection with level 2 client authentication, which passes the client certificate to the MVS host TN3270 server. The MVS host TN3270 server uses RACF Secured Signon services to obtain a user ID and PassTicket.

The two-tier design is supported in z/OS V1R2 and OS/390 V2R10 with PQ47742 (UQ55691).

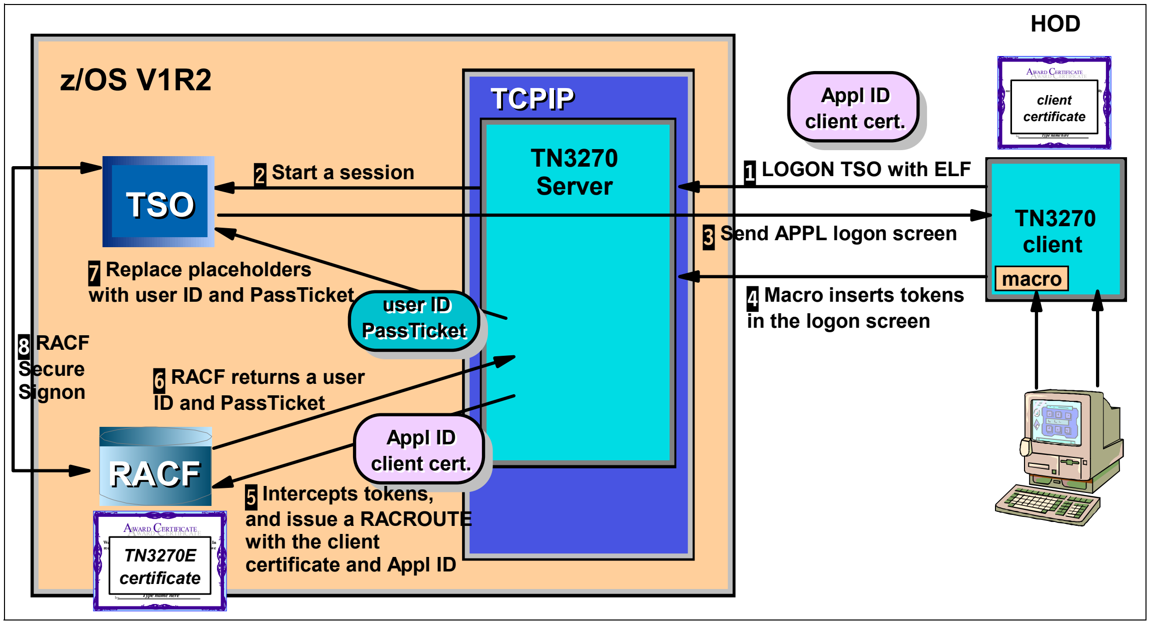


Figure 15-9 Certificate Express Logon two-tier network design

Here are the steps when a client wants to access a TSO session on z/OS:

1. The user has a Host On-Demand icon that starts an emulator session configured to use SSL client authentication. The session has a macro associated with it. A client certificate has to be available from the terminal and presented to the TN3270 server for the SSL handshake. During the SSL handshake, the client certificate is passed to the TN3270 server and validated. During Telnet function negotiation, the Certificate Express Logon capability is negotiated using RFC 1572.
2. The application ID is sent from the client to the TN3270 server and the server starts the session with TSO.
3. The logon screens come to the emulator.

4. The macro plays and inserts placeholder strings in the user ID and password fields.
5. The TN3270 Server intercepts the placeholder strings and sends the certificate and the target application ID to RACF.
6. RACF converts the Host On-Demand client's certificate to a TSO user ID and PassTicket, and sends them back to the TN3270 server.
7. The TN3270 server inserts the user ID and PassTicket into the 3270 data stream at the macro-inserted placeholder locations, and sends it to the application.
8. The application presents the user ID and PassTicket to RACF or other compatible host access control facility, which approves them and the logon completes as usual.

Three-tier network design

In the three-tier design, the user starts the TN3270 connection to the middle-tier server.

There must be a Digital Certificate Access Requestor (DCAR) and a Digital Certificate Access Server (DCAS).

A Digital Certificate Access Server (DCAS) resides on the host. DCAS uses RACF services to obtain a user ID. A DCAR is the part of the TN3270 middle-tier server that supports the Certificate Express Logon and communicates as a client with the DCAS. It is not separate from the TN3270 middle-tier server.

The DCAS's client is the middle-tier TN3270 server or DCAR, which attempts to log on to an SNA application for the workstation client. The DCAS receives a digital certificate from the DCAR and returns a user ID and PassTicket. SSL communication is used between the DCAS and the DCAR. The server recognizes that the client wants the Certificate Express Logon and invokes the DCAR, which opens an SSL connection with client authentication and passes the workstation's certificate and application name to the DCAS on the host. The DCAS uses RACF Secured Signon services to obtain a user ID and PassTicket, which the DCAS returns to the DCAR. The DCAR passes this information back to the TN3270 server.

The middle-tier IBM TN3270 servers supporting Certificate Express Logon are:

- Communications Server for OS/2 Warp V6.1
- Communications Server for Windows NT and Windows 2000 V6.1.1 PTF
- Communications Server for AIX 6.0.0.1 PTF

The host also provides RACF Secured Signon services, which the DCAS or the MVS host Telnet server uses to generate a PassTicket. A PassTicket is a RACF token similar to a password except that it is valid only for ten minutes.

In review, the three-tier components are (refer to Figure 15-10):

- A client workstation that supports Secure Sockets Layer (SSL) connections with client authentication and an X.509 certificate.
- A middle-tier TN3270 server, so called because it does not reside on the host, but rather between the client and the host. The Digital Certificate Access Requestor (DCAR) resides on this server. DCAR communicates with a DCAS using an SSL connection with client authentication. It sends the user's certificate from the workstation and an application ID to the DCAS, and expects to receive a user ID and PassTicket (a one-time password) in response. This is the user ID and password that will be used to log on to the SNA application.
- The Digital Certificate Access Server (DCAS) resides on the host. The DCAS uses RACF services to obtain a user ID that is associated with the certificate sent by the client. RACF also provides secured sign-on services, which the DCAS uses to generate a PassTicket. A PassTicket is a RACF token similar to a password except that it is valid only for 10 minutes.

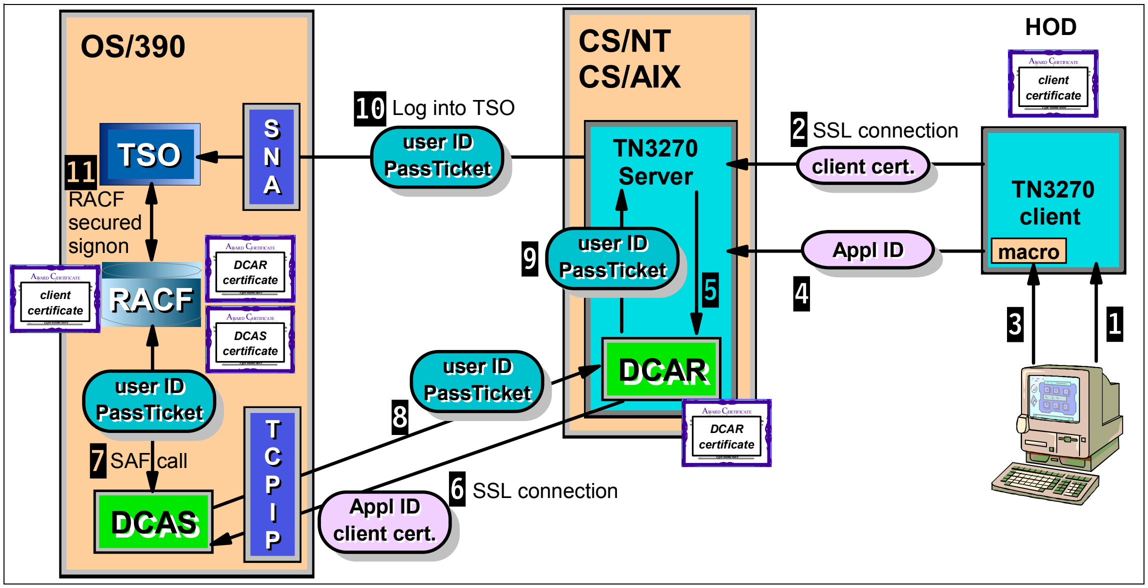


Figure 15-10 Certificate Express Logon three-tier network design

The SNA connection between the TN3270 server and SNA application can be SNA LU2, DLUR, HPR/IP (Enterprise Extender - EE), or AnyNet connection.

The Secure Sockets Layer (SSL) communication with client authentication is required in the configuration of the Certificate Express Logon on the Host On-Demand client, TN3270 server, and OS/390 DCAS server.

The following describes the example shown in Figure 15-10 where the client wants to access a TSO session on a z/OS host:

1. The user references a Host On-Demand HTML page that downloads the Host On-Demand code (or loads the cached client from its local disk) and starts an emulator session. The session definitions are retrieved either from Host On-Demand's configuration server, or directly from the HTML page referenced. The session definitions must specify that this session uses SSL encryption with client authentication and a Certificate Express Logon macro must be available to the user. The certificate file is unlocked with a PIN and the user's (X.509) certificate is retrieved to be used during the SSL handshake flows.
2. The Host On-Demand client starts a TN3270 connection to its TN3270 server requesting SSL encryption with client authentication using an X.509 certificate. The certificate is sent to the TN3270 server and, after having been validated, is saved for later reference at the TN3270 server for this session. During the Telnet function negotiation, the Certificate Express Logon is agreed upon using the handshake protocol described in RFC 1572.
3. A macro recorded for this session supporting the Certificate Express Logon is started either explicitly by the user or automatically when the host connection is initialized. Before recording the macro, an application ID had to be specified for this macro. This application ID must be the name under which the destination application is known to RACF on the application host.
4. The application ID is sent to the TN3270 server using the Telnet handshake protocol in order to make the TN3270 server aware of which application the user intends to connect to using a Certificate Express Logon macro. The logon macro is then played and eventually the host application sends the screen(s) designed to prompt for user ID and password (can be on different screens). Instead of filling in a previously recorded user ID and password or prompting the user to provide them in a separate window (as normal macro processing would be), the macro inserts placeholder strings into the fields for user ID and password ($USR.ID$ and $PSS.WD$, respectively).

   The TN3270 server intercepts the screens prompting for user ID and password until it can replace the placeholder strings with a valid user ID and password.
5. If this is the first user requesting assistance for Certificate Express Logon, the TN3270 server invokes the Digital Certificate Access Requester (DCAR) function to establish a secure and trusted TCP/IP connection to its configured Digital Certificate Access Server (DCAS) using SSL V3 for encrypting the

data exchange flows. If this connection has already been established for an earlier request, the existing connection is used.

6. On this secure SSL connection, the TN3270 server sends a request for a user ID and PassTicket providing the destination application ID and the user's certificate (that was saved for this session during connection establishment).
7. DCAS is a function of Communications Server for OS/390 and z/OS and interacts with RACF on the host to verify the validity of the user's certificate. Only certificates for which a user ID has been defined are accepted. If the certificate's associated user ID is, in addition, authorized to access the requested application, a PassTicket is generated and, together with the user ID, returned to DCAS. The DCAS server makes SAF calls to convert the Host On-Demand client's certificate to a TSO user ID and PassTicket.
8. The user ID and PassTicket are sent to the TN3270 server over the secure (SSL-encrypted) TCP/IP connection in response to the previous request.
9. The DCAR function passes the user ID and PassTicket to the TN3270 server for placement into the logon datastream.
10. The TN3270 server then replaces the placeholder variable for the user ID ($USR.ID$) on the withheld host logon screen and releases the screen for transmission over the SNA LU-LU session towards the host application. It subsequently also replaces the placeholder variable ($PSS.WD$) for the password with the PassTicket when the host screen requesting the password shows up, if it is not already replaced on the primary logon screen together with the user ID.
11. The host application presents user ID and PassTicket (received in the 3270 data stream) to RACF in order to check if the user is authorized to log on to this application. The PassTicket should still be valid (unless you have severe performance problems in your system) and RACF will then grant access to the application.

15.2.2 Planning for Certificate Express Logon

To use Certificate Express Logon, the following actions are required:

- The host session must be configured for SSL with client authentication.
- The connection must be to one of the supported Telnet servers.
- Each user must have his own unique digital certificate because Certificate Express Logon and RACF will associate each digital certificate to the user's RACF user ID and password.
- You must record a macro that the user will use to log on to the host application. The macro record function steps you through the process for creating an Certificate Express Logon macro.

- Distribute that macro to the clients.

Some configuration needs to be done on the Telnet servers and on the iSeries system that you are accessing. The information in this book will assist you in configuring the Host On-Demand component. For a complete tutorial and examples of all supported platforms, refer to:

```
ftp://ftp.software.ibm.com/software/network/library/whitepapers/elf.pdf
http://www-3.ibm.com/software/network/library/whitepapers/elf.html
```

For additional configuration information, you may also refer to the documentation for the server platform you have implemented:

- Communications Server for OS/2 Warp - What’s New
- Communications Server for Windows NT - Readme file
- Communications Server for AIX - Readme file
- Communications Server for OS/390:
  - *z/OS V1R1.0 CS: IP Migration*, SC31-8773

Refer to 3.7, “Certificate Express Logon” on page 112 for details on how to set up the zSeries for Certificate Express Logon.

15.2.3 Host On-Demand session setup

Before you can start recording a macro using the Certificate Express Logon, you have to define a session that is able to provide Certificate Express Logon support. When recording the macro, the session definitions are not checked, that is, you can record a macro for Certificate Express Logon support that might not work correctly when played.

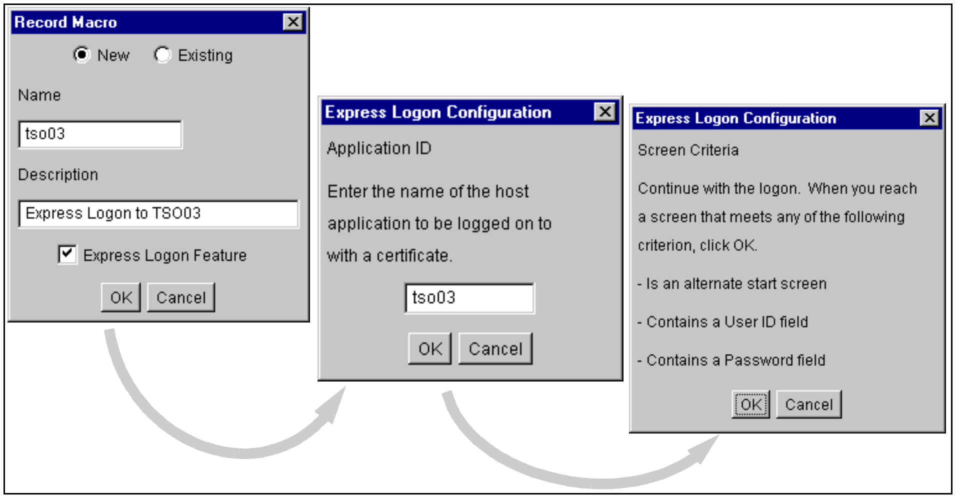
The session must be configured for SSL and client authentication. A client certificate must have been installed on the client or must be accessible from a server. The destination IP address must specify a server that has been set up to support the Certificate Express Logon.

> **Note:** If the connection to the TN3270 server is through the Host On-Demand Redirector or the Communications Server for AIX Telnet Redirector, the security option for the Redirector must be set to `pass-through`.

Refer to 7.1.7, “Configuring sessions” on page 277 for details on how to configure the Host On-Demand client sessions.

15.2.4 Record the Logon macro

Recording the macro is started the normal way by clicking **Record** on the session window’s toolbar or by selecting **Actions -> Record Macro**. The session itself may have been started from a client by logging in as a user and then opening the intended session window. You may also record a Certificate Express Logon macro as an administrator customizing an HTML page that, when referenced, automatically opens the session window, starts the macro, logs the user on to his host application, and navigates the user to the application’s start window.



● New ○ Existing

Name: tso03

Description: Express Logon to TSO03

☑ Express Logon Feature

Application ID

Enter the name of the host application to be logged on to with a certificate.

tso03

Screen Criteria

Continue with the logon. When you reach a screen that meets any of the following criterion, click OK.

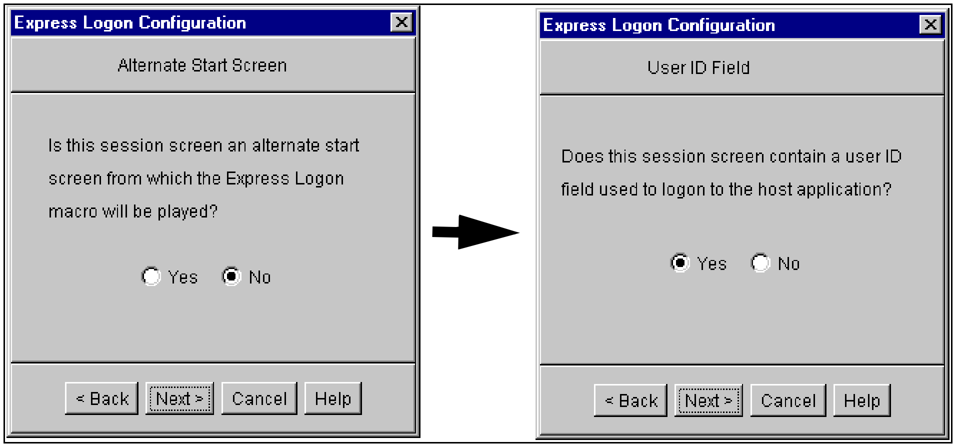
- Is an alternate start screen
- Contains a User ID field
- Contains a Password field

Figure 15-11 Recording the Certificate Express Logon macro - getting started

Figure 15-11 shows the sequence of the first three windows that appear when you start recording a Certificate Express Logon macro. On the first window you have to specify the name of the new macro (of course, you may also append to or overwrite an existing macro). Select the **Certificate Express Logon** check box to indicate that you want to use Certificate Express Logon. Clicking **OK** causes the second window in Figure 15-11 to appear, prompting you to enter the application ID of the application you are logging on to with this macro. This is the name of the application that was used when it was defined to RACF on the OS/390 host.

After having entered the application ID and clicking **OK**, the third window in Figure 15-11 appears, prompting you to actually start recording your actions on the session window. Once you have reached the window prompting you for the user ID, click **OK** on the third window in Figure 15-11.

The next window (Figure 15-12) then will ask if this is an alternate start window.



Express Logon Configuration

Alternate Start Screen

Is this session screen an alternate start screen from which the Express Logon macro will be played?

○ Yes ● No

Express Logon Configuration

User ID Field

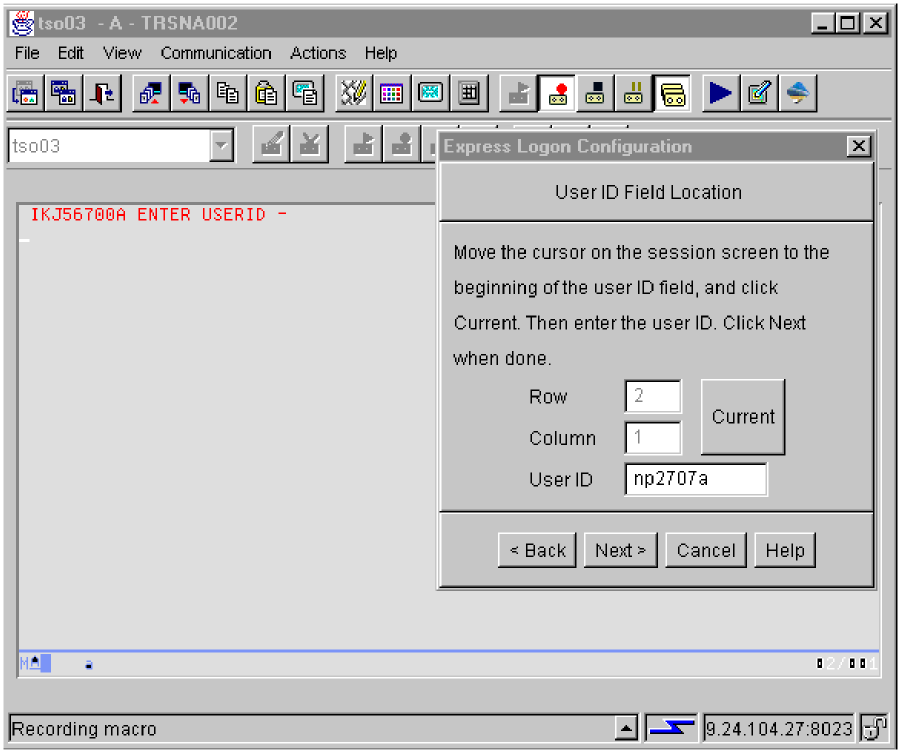
Does this session screen contain a user ID field used to logon to the host application?

● Yes ○ No

Figure 15-12 Recording the Certificate Express Logon macro - getting to the user ID field

You can define alternate start windows, which can be more than one, in the first or a follow-on editing pass through the macro. This will allow the user to start the macro (or have it started automatically) when the host session is initialized. After having logged off from the application, a different logon window might be presented to the user (for example, the application's logon window and not VTAM's USSMSG10). This then will allow the user to use the same macro for one application, independent of where he starts.

The next window, when not defining an alternate start window, asks if there is a user ID field on the current host window. Clicking **Yes**, then **Next** from the following window leads you to a window that lets you define the position of the user ID field on the host window. See Figure 15-13.



IKJ56700A ENTER USERID -

Express Logon Configuration

User ID Field Location

Move the cursor on the session screen to the beginning of the user ID field, and click Current. Then enter the user ID. Click Next when done.

Row: 2
Column: 1
User ID: np2707a

Recording macro

9.24.104.27:8023

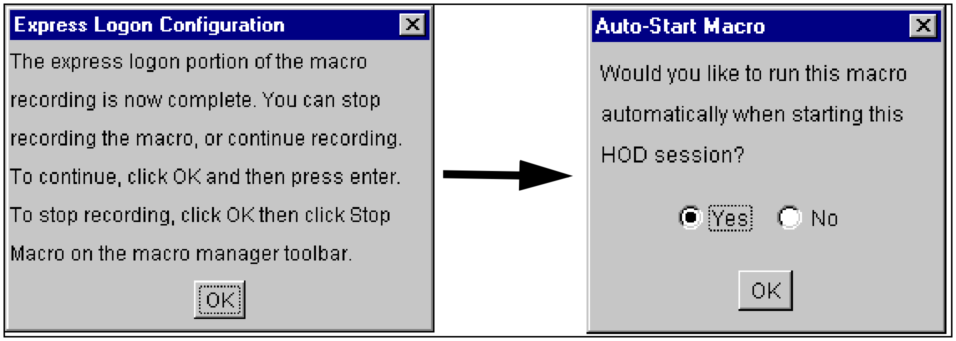
Figure 15-13 Recording the Certificate Express Logon macro - user ID field

The simplest way of getting the correct row and column is by positioning the cursor on the user ID input field (normally, it will already be correctly positioned) and clicking **Current**. This will update the input fields in the window with the current cursor position. In the user ID field, fill in a valid user ID. This user ID then will only be used to log on to the host application while recording the macro; it will not be recorded in the macro. Instead, a placeholder variable, `)USR.ID(`, will be placed in the macro and actually filled into the host window's user ID field when the macro is played. The TN3270 server then will replace this variable with the user's correct user ID.

The next window presented will ask if there is also a password field on the host window that prompts for the user ID. If you answer yes, the password field is on the same window as the user ID field, or after having navigated to the window prompting for the password, you have to define the position of the password field on a window similar to the one used for the password field as shown in

Figure 15-13. Also, the password you are entering here is not recorded in the macro. It is only used to actually log on when recording the macro. The macro will again contain the placeholder variable, `)PSS.WD(`, that will be replaced with the PassTicket by the TN3270 server when playing the macro.

When you click **Finish**, the left window shown in Figure 15-14 is displayed giving instructions on how to continue. Only when you really want the user to press the Enter key, or whichever PF key is used for the logon, do you follow the instructions to stop the macro immediately. Otherwise, click **OK** to remove the window and continue recording your macro until you have reached the application’s start window where you want to leave the user.



The express logon portion of the macro recording is now complete. You can stop recording the macro, or continue recording. To continue, click OK and then press enter. To stop recording, click OK then click Stop Macro on the macro manager toolbar.

Would you like to run this macro automatically when starting this HOD session?

● Yes ○ No

Figure 15-14 Recording the Certificate Express Logon macro - finishing steps

When you stop recording the macro, a final window (shown on the right in Figure 15-14) will appear asking you whether you want this macro to be automatically started when the session window is initialized. If you click **Yes**, the corresponding session definitions will be updated.

Important: The initial release of Certificate Express Logon (known as the Express Logon Feature) used the variables `$USR.ID$` and `$PSS.WD$`. However, because of national language translation issues, these variables were changed to `)USR.ID(` and `)PSS.WD(`. This change for Host On-Demand was introduced in Version 5.0.4. The following releases of the mid-tier communications servers support the new variables:

- Communications Server for OS/2 V6.1
- Communications Server for Windows NT and Windows 2000 V 6.1.1
- Communications Server for AIX V 6.0.0.1

16

Web Start

The Java Web Start client feature enables users to start Host On-Demand sessions without a browser. Users require only a Java Runtime Environment and Web Start installed on their computers. Using this feature, Host On-Demand sessions run as a Java application, independent from a browser.

In this chapter, we will discuss Web Start clients including the following topics:

- Overview of Web Start client
- Installation and configuration
- Uninstalling
- Limitations

16.1 Overview of Java Web Start

In previous versions of Host On-Demand, clients use a HOD session, which is launched in a browser. Because of this, users must be careful, for example, to not terminate the browser while the Host On-Demand session is running.

The Java Web Start client feature in Host On-Demand V8 makes it possible to use HOD sessions independent from browsers, or even without using browser.

This function provides a Host On-Demand session as a Java 2 cached client, and installs it on the client machine. There is no support for Database On-Demand, administrative clients, or the NewUser applet. In addition, because Web Start is a Java application on the client machine, you cannot use it for HTML Override or with JavaScript API.

16.1.1 What is Java Web Start?

Java Web Start is a technology that makes it possible for Java applications to be distributed over the network. Unlike applets which must be accessed with a browser and depend on the browser JVM, Java Web Start runs as a Java application, independently of any browser.

With a Host On-Demand client using the Java Web Start feature, you can distribute HOD client code over the network, and run it without any browser as a Java application.

For more information on Java Web Start, refer to the following Web sites:

http://java.sun.com/product/javawebstart/
http://java.sun.com/j2se/1.4.2/docs/guide/jws/developersguide/contents.html

16.2 The Java Web Start client

There is no default Java Web Start client page provided with Host On-Demand. The HOD administrator must prepare for Web Start by using the Deployment Wizard to create Web Start clients. The Deployment Wizard generates a Java Network Launch Protocol (JNLP) file, an HTML file (which will invoke the JNLP file), and files for session configuration. The following is an example of files generated, where `myWSclient` is the name of file specified in the Deployment Wizard:

- myWSclient.html
- myWSclient.jnlp
- HODData/myWSclient/cfg0.cf
- HODData/myWSclient/params.txt

- HODData/myWSclient/policy.obj
- HODData/myWSclient/preloads.obj
- HODData/myWSclient/wInfo.txt

16.2.1 Starting a Web Start client

There are several ways you can start a Web Start client:

- It can be started from a client browser pointing to the HTML file (myWSclient.html in the previous example).
- It can be started from the JNLP file (myWSclient.jnlp in the previous example).
- You can also start it from Web Start Application Manager (a component of Java Web Start).

We will discuss various ways to install and start a Web Start client later in this chapter (16.4.1, “Web Start client installation” on page 602).

Every time a user accesses the JNLP file (or the HTML file, which eventually points to JNLP file) to start a Web Start client, a splash screen is displayed in Figure 16-1.

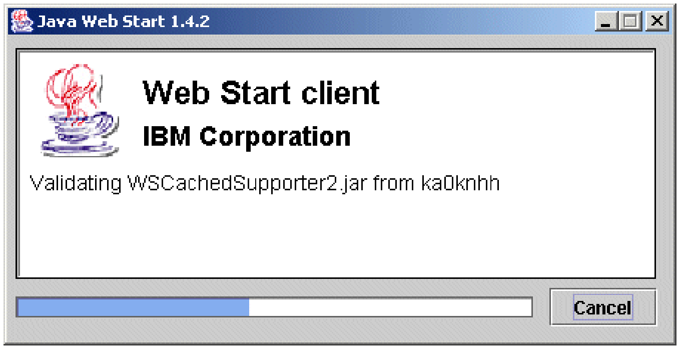
Web Start client

IBM Corporation

Powered by Java(tm) Web Start

Figure 16-1 Web Start client splash with Java Web Start 1.2

It will search the client machine to see if the client code already installed. If not (for example, the first time the code is accessed on the Host On-Demand server), the client code will be downloaded and cached.



Validating WSCachedSupporter2.jar from ka0knhh

Figure 16-2 Downloading archives for Web Start client

When you launch a Web Start client, the following three files are started:

- WSCachedSupporter2.jar
- CachedAppletInstaller2.jar
- WSCachedLoader2.jar

They are responsible of keeping HOD code on the client machine up to date. If there is a newer version on the Host On-Demand server, the new code will be downloaded.

After checking the version and downloading code, Java Web Start will launch the session and actual Host On-Demand code runs. It is similar to the normal Java 2 cached client. However, with Java Web Start, the HOD code runs as a Java application.

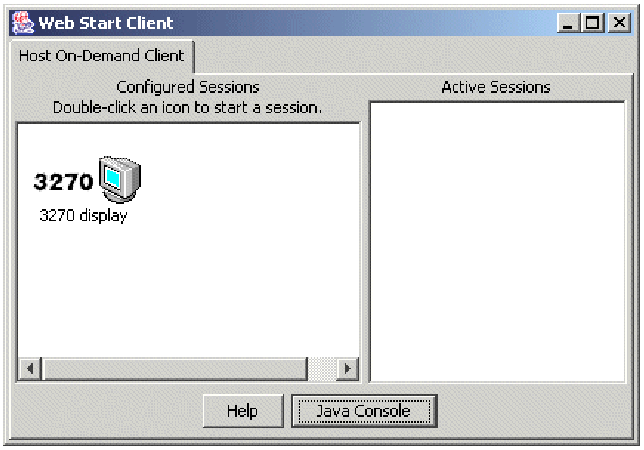
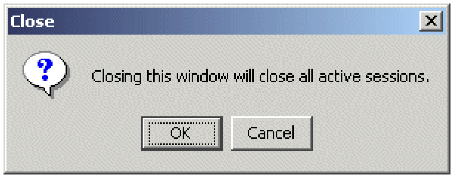


Figure 16-3 Example of a Web Start client

After the first time a client is launched, the client will check to see if there are files to update every time you launch the session. (For information on start up of the client, refer to 16.4.2, “Launching the Web Start client after initial installation” on page 605).

Using Web Start clients, Host On-Demand sessions do not depend on a browser. They are launched as a Java application. Therefore, closing a browser does not end a Host On-Demand session.

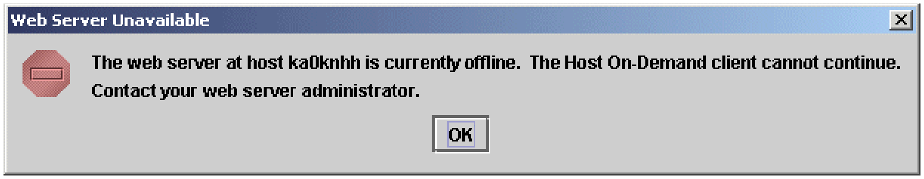
If the user attempts to close the Host On-Demand desktop with active sessions running, the user will be prompted to make sure they want to close all sessions (Figure 16-4). If so, the sessions are terminated cleanly to prevent problems that occur when there are sessions running in the browser, and the browser is abruptly closed.


Close

Closing this window will close all active sessions.

Figure 16-4 Error message while Host On-Demand session is running

Host On-Demand Web Start clients need to have a Web server (where the JNLP file code base is located) running when they start up. If the Web server is down, you will receive a Web Server Unavailable prompt, and will not be able to start Web Start clients until the Web server is started.


Web Server Unavailable

The web server at host ka0knhh is currently offline. The Host On-Demand client cannot continue. Contact your web server administrator.

Figure 16-5 Web Server Unavailable prompt

16.2.2 Considerations when using a Web Start client

The following considerations should be kept in mind when planning for Web Start clients:

- Java Web Start is bundled with JRE 1.4. If you use JRE 1.3, you must either download Java Web Start, or upgrade to JRE 1.4. These can be downloaded from:
  `http://java.sun.com/`

- Windows Restricted Users require Web Start 1.2 (which is bundled with Sun JRE 1.4 and above or IBM JRE 1.4.1) installed on a machine. Web Start 1.0.1 does not support Windows Restricted Users.

> **Note:** Host On-Demand V8 is shipped with IBM JRE 1.4.0, which includes Java Web Start V1.0.1.

- The Host On-Demand Web Start client has the following requirements:
  - JRE 1.4 or later is required to use HTTPS to access files from the Web server.
  - JRE 1.4 or later is required to use an HTTP proxy with Web Start.
  - Session properties that use browser settings (such as proxy server or TLS/SSL) cannot be used with Web Start.
  - Mac OS X with a wide screen laptop has a JRE problem (inverted title bar).
- Because Web Start clients are launched independently from browsers, the following limitations apply:
  - Web Start clients are not compatible with the Portal Server.
  - Web Start clients cannot be used with an HTML template or JavaScript Session Manager API.
- Web Start clients are supported only for the Java 2 Cached client. There is no Web Start client support for Administrative clients, Database On-Demand clients, and New Users applet.

16.3 Preparing for Web Start clients

In this section, we discuss preparation needed to start Web Start clients.

16.3.1 Preparing the Web server

In order for clients to download files needed from Host On-Demand Server and launch Web Start client, administrators will need to add Java Network Launch Protocol (JNLP) files to MIME types of Web Servers.

Apache HTTP Server or IBM HTTP Server

Add following line to conf/mime.types:

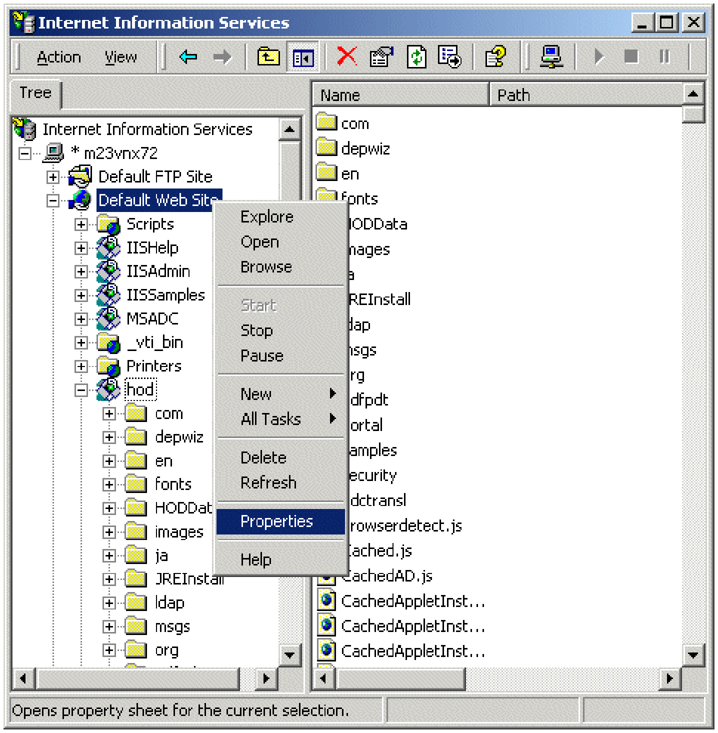
```
application/x-java-jnlp-file JNLP
```

Microsoft IIS 5.x

Complete following steps:

1. From the control panel, open **Administrative Tools -> Internet Services Manager.**
2. Open **Internet Information Services -> host01**, where your hostname is host01.
3. Select **Default Web Site**, right-click to select **Properties.**

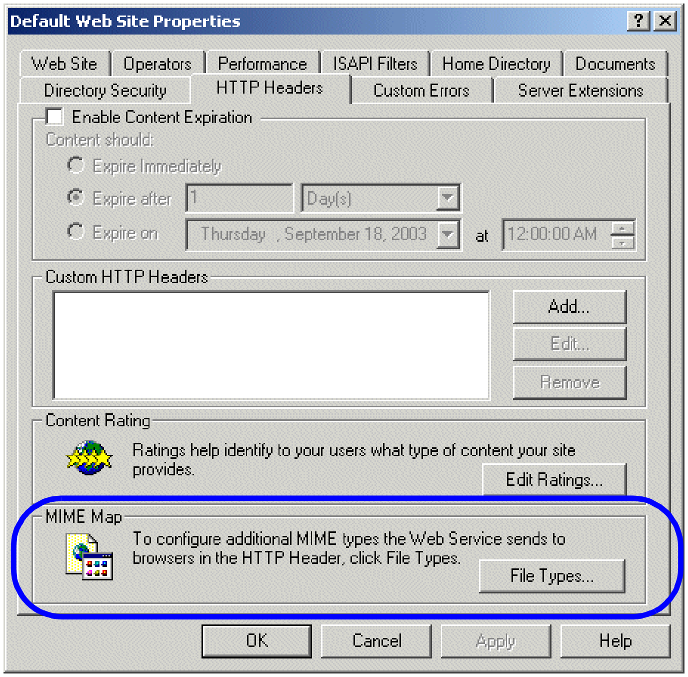
   You can set MIME type by various levels within your server. For example, you can limit this setting to a certain alias, such as `hod`, or apply it to entire Web site on the server (refer to Figure 16-6). Therefore, instead of selecting **Default Web Site**, you can choose your hostname or hod alias to expand or limit this setting.



Opens property sheet for the current selection.

Figure 16-6 Internet Information Services panel

4. Click the **HTTP Headers** tab on the Properties window. The window shown in Figure 16-7 will be displayed.



□ Enable Content Expiration

Content should:

○ Expire Immediately

● Expire after 1 Day(s)

○ Expire on Thursday , September 18, 2003 at 12:00:00 AM

Ratings help identify to your users what type of content your site provides.

To configure additional MIME types the Web Service sends to browsers in the HTTP Header, click File Types.

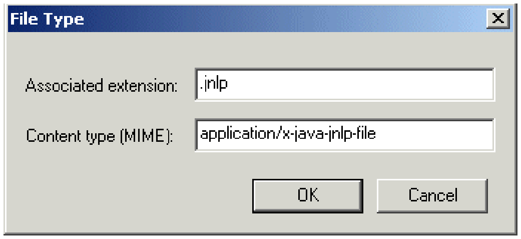
Figure 16-7 IIS - Default Web Site Properties

5. Under MIME Map, click **File Types...**.

6. Click **New Type...**.

7. Input following values:

   – **Associated extension**: .jnlp
   – **Content type (MIME)**: application/x-java-jnlp-file

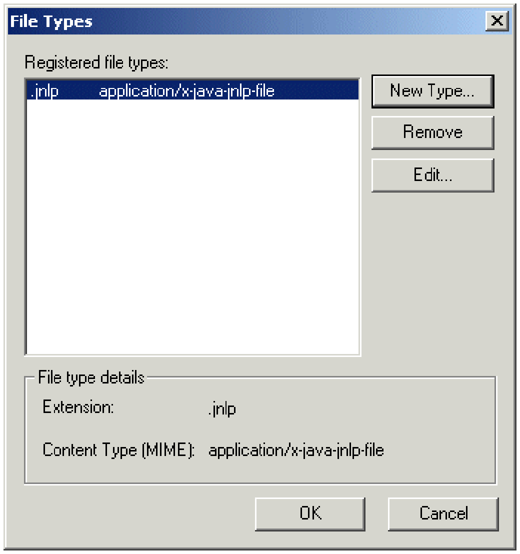


Associated extension: .jnlp

Content type (MIME): application/x-java-jnlp-file

Figure 16-8 Setting the file type

8. Click **OK**.



.jnlp application/x-java-jnlp-file

Extension: .jnlp

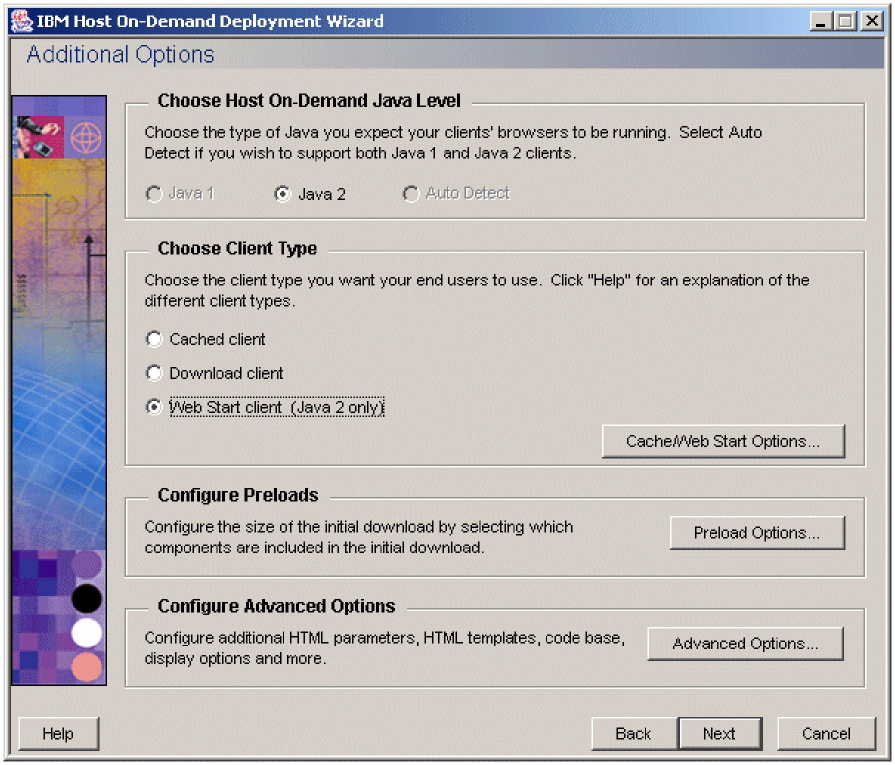
Content Type (MIME): application/x-java-jnlp-file

Figure 16-9 After .jnlp is added to the entry

Be sure that you set the correct MIME type for each Web server. Otherwise, you might see .jnlp files in text form when you access to the file.

16.3.2 Creating files for a Web Start client

Host On-Demand administrators must use the Deployment Wizard to create HTML files configured for Web Start client support. Web Start clients support all configuration models (HTML-based model, Configuration server-based model, and Combined model) that can be generated using the Deployment Wizard.


IBM Host On-Demand Deployment Wizard
Cache/Web Start Options...
Preload Options...
Advanced Options...
Help
Back
Next
Cancel

Additional Options

Choose Host On-Demand Java Level

Choose the type of Java you expect your clients' browsers to be running. Select Auto Detect if you wish to support both Java 1 and Java 2 clients.

○ Java 1 ● Java 2 ○ Auto Detect

Choose Client Type

Choose the client type you want your end users to use. Click "Help" for an explanation of the different client types.

○ Cached client

○ Download client

● Web Start client (Java 2 only)

Configure Preloads

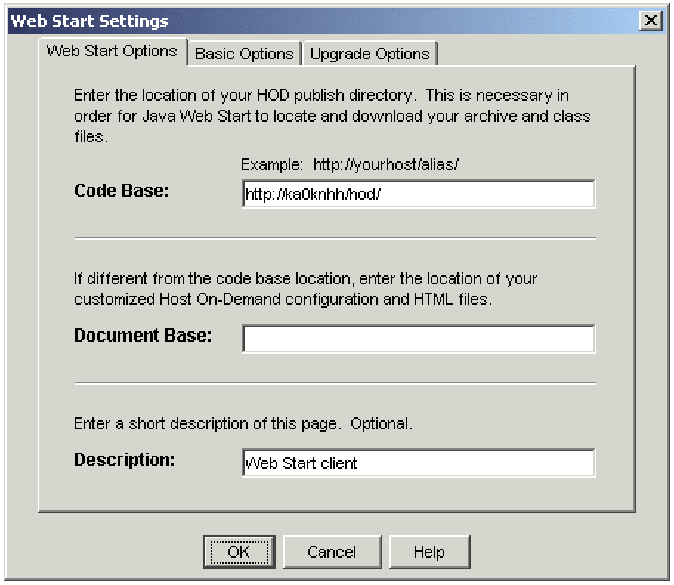
Configure the size of the initial download by selecting which components are included in the initial download.

Configure Advanced Options

Configure additional HTML parameters, HTML templates, code base, display options and more.

Figure 16-10 Advanced option panel on Deployment Wizard

When you select Web Start as your client type on the Additional Options window in the Deployment Wizard (Figure 16-10), the Web Start Settings window launches. See Figure 16-11.



Enter the location of your HOD publish directory. This is necessary in order for Java Web Start to locate and download your archive and class files.

Example: http://yourhost/alias/

Code Base: http://ka0knhh/hod/

If different from the code base location, enter the location of your customized Host On-Demand configuration and HTML files.

Document Base:

Enter a short description of this page. Optional.

Description: Web Start client

Figure 16-11 Setting Codebase in Deployment Wizard

You will need to set the Code Base to where you installed the Host On-Demand server code with the HOD alias. For example, if you installed Host On-Demand server on machine named `ka0knhh` with the alias set to `hod`, you will need to set to `http://ka0knhh/hod/.` See Figure 16-11.

In addition, if you keep customized HTML files in a directory different from the Code Base, you will need to specify this as well in Document Base.

At the completion of the Deployment Wizard, you can only choose HTML or ZIP files for the output format. Web Start clients are not compatible with JavaScript API nor the Portal Server.

16.4 Installation of the Web Start client

The Host On-Demand Web Start client is similar to a cached client in that the client code must be downloaded and installed (cached) on the client system the first time it is used. In this section, we discuss the installation of the HOD Web Start client.

16.4.1 Web Start client installation

When you access a Web Start client for the first time, you must install it on your client system. You have three options to install the Web Start client:

- From a Host On-Demand Server with a browser
- From a Host On-Demand Server without a browser
- From a LAN drive or CD drive

Installing from a Host On-Demand server with a browser

To install the Web Start client from a Host On-Demand server, you must specify the full URL of the HTML file in your browser. For example:

```
http://<server_name>/<hod_alias>/WSclient.html
```

where WSclient.html is the HTML file you want to load.

You can also point to the JNLP file, which is launched from the HTML file.

```
http://<server_name>/<hod_alias>/WSclient.jnlp
```

The Web Start client begins installing immediately. A window shows the progress of the installation. The upper progress bar of this window shows the status of individual files as they download, while the lower progress bar shows the status of the overall installation.

When the installation completes, the installation code immediately launches the Web Start client in a separate window from the browser. The user does not have to restart the browser.

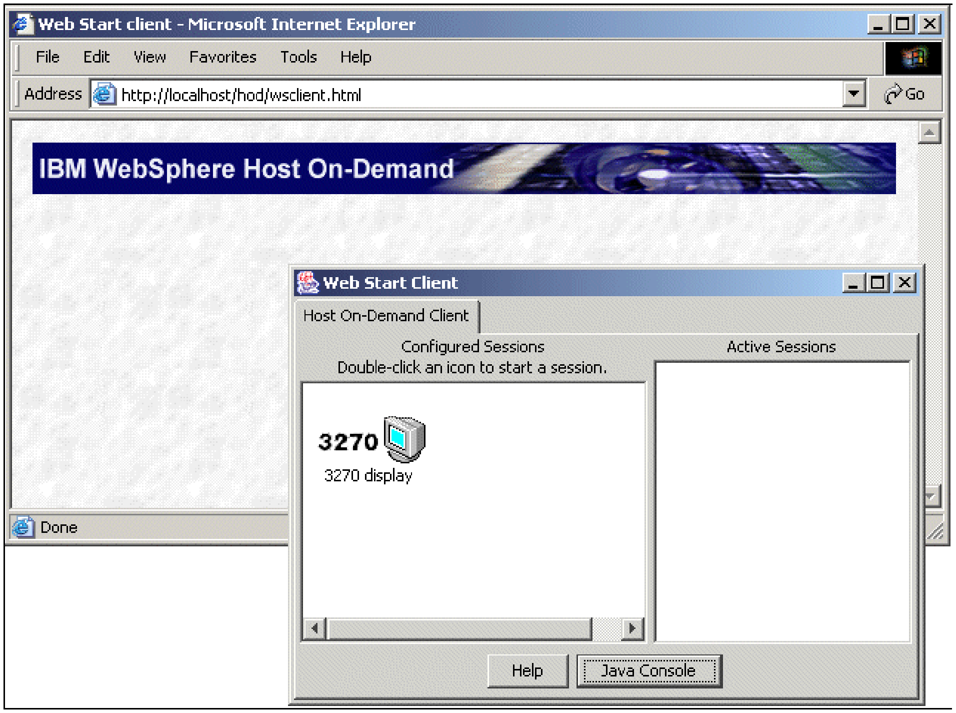
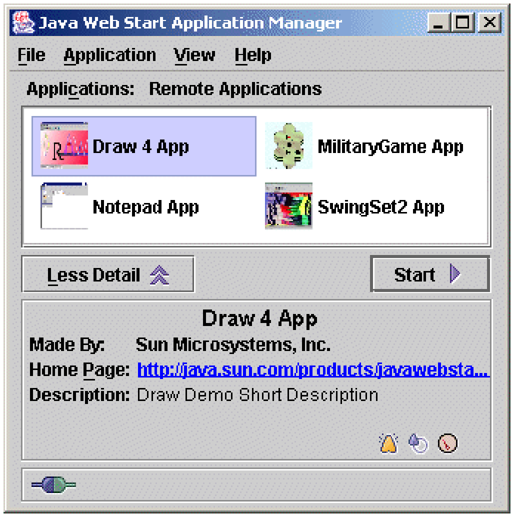

Web Start client - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost/hod/wsclient.html
Go
IBM WebSphere Host On-Demand
Web Start Client
Host On-Demand Client
Configured Sessions
Double-click an icon to start a session.
Active Sessions
3270
3270 display
Help
Java Console
Done

Figure 16-12 Launching the Web Start client by accessing HTML file

Installing from a Host On-Demand Server without a browser

You can install Web Start client without using a browser. All you need is to distribute JNLP files to client machines or to LAN drives, where users can access them. Users can start installation by accessing this file. Installation will start immediately.

After you have accessed the JNLP file the first time and installed the Web Start client, you can start the client from the Java Web Start Application Manager (WSAM). WSAM is a component of Java Web Start. It maintains information on all Web Start applications. You can start WSAM from the Web Start icon on your desktop.


Java Web Start Application Manager
File Application View Help
Applications: Remote Applications
Draw 4 App
MilitaryGame App
Notepad App
SwingSet2 App
Less Detail
Start

Draw 4 App
Made By: Sun Microsystems, Inc.
Home Page: http://java.sun.com/products/javawebsta...
Description: Draw Demo Short Description

Figure 16-13 Java Web Start Application Manager

Windows users can use a command to start installing a Web Start client. The command is

```
start myhod.jnlp
```

where the name of JNLP file is `myhod.jnlp`. In this case, you need the JNLP file copied to the client machine. If you chose to create an icon, a Host On-Demand icon will be created on desktop. The user can double-click this icon to launch the Host On-Demand session.

Installing from LAN drive or CD drive

Some or all of your users can initially download the Web Start client from a LAN drive or CD. The user is required to access the LAN drive or CD only once to install the Web Start client. Afterwards, the user connects to the Host On-Demand server as usual.

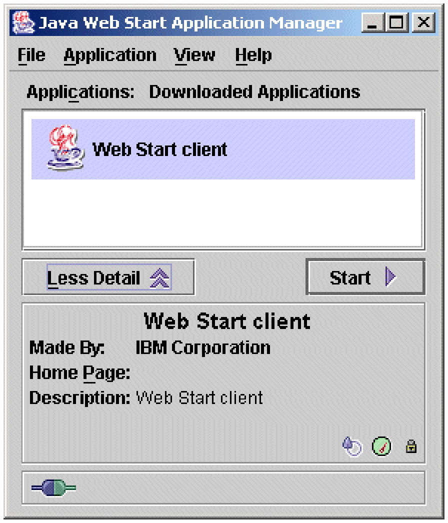
When installing from a LAN or a CD, the Web Start components are installed on the user's workstation more quickly than if they were downloaded from the Host On-Demand server. In addition, the user is not placing an additional load on the Host On-Demand server by downloading an entire set of Web Start client components, as long as they are at same level.

For additional information, refer to *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301.

16.4.2 Launching the Web Start client after initial installation

After initial installation of the Web Start client, you can launch the client using a browser and the same HTML, or JNLP file for all subsequent session requests. In addition, there are several other ways to launch the Web Start client.

One way to start a session is from the Java Web Start Application Manager. You can start it by selecting the Web Start client and click the **Start** button, or choose **Application** -> **Start Application.**



Web Start client

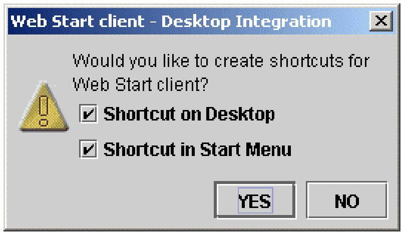
Made By: IBM Corporation

Home Page:

Description: Web Start client

Figure 16-14 Java Web Start Application Manager example

If you are using the default settings for Java Web Start, you will be asked if you want to add a shortcut to desktop and in the start menu. See Figure 16-15.



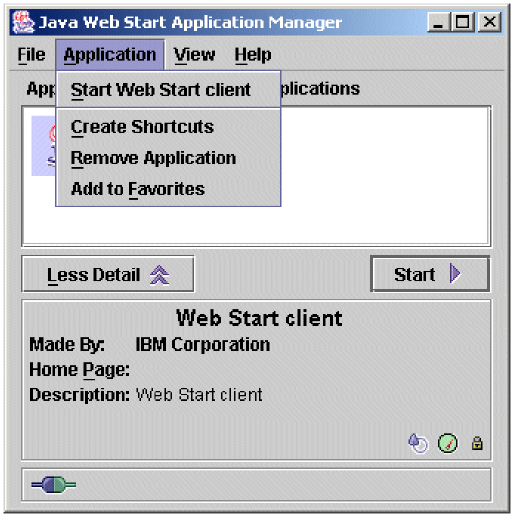
Would you like to create shortcuts for Web Start client?

☑ Shortcut on Desktop

☑ Shortcut in Start Menu

Figure 16-15 Pop-up for adding icon and entry for Start menu

There is another way to add a shortcut to the desktop or in the start menu. That is from Java Web Start Application Manager. Select the Web Start client and go to **Application** -> **Create Shortcuts**.



Web Start client

Made By: IBM Corporation

Home Page:

Description: Web Start client

Figure 16-16 Adding shortcuts from WSAM

You can also start session from shortcuts.

After Web Start is restarted, it checks the Host On-Demand server for updates to the archives and downloads any updated files, just like cached clients.

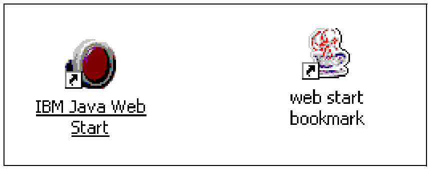


Figure 16-17 Example of Web Start desktop icon (JWS 1.0.1 and JWS 1.2)

16.5 Customizing Web Start clients

In this section, we discuss using Web Start clients.

16.5.1 Updating the Web Start client

After the initial install of the Web Start client, if users point their browsers to the HTML file generated by the Deployment Wizard, and there are updates available on the Host On-Demand server, Host On-Demand prompts the user to update the client. If the user allows the update, Java Web Start downloads the updated archive files and launches Host On-Demand. If the user declines to upgrade, Host On-Demand prompts the user again the next time he launches the HTML file.

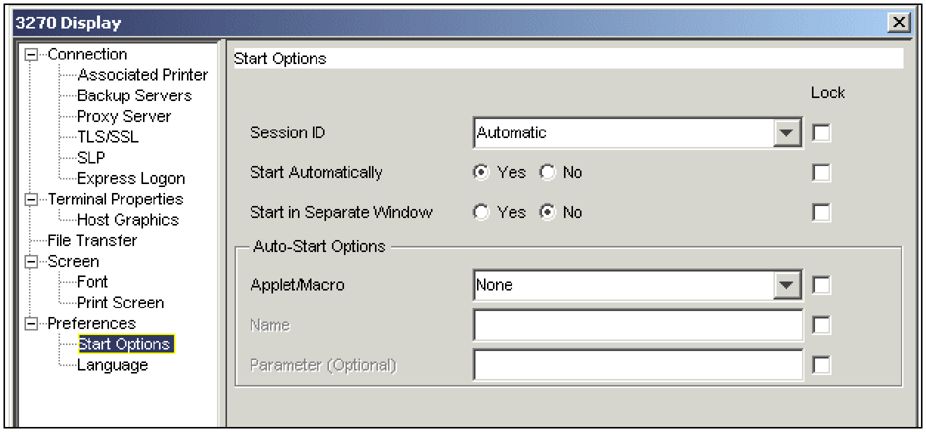
Adding Web Start components after the initial install

If users request a function that is not installed on the Java Web Start client, Host On-Demand prompts them to install the additional components required for that function. If they choose to install the additional components, they must restart Web Start client after completing the download to use those function.

16.5.2 Bookmarking sessions with Web Start

Since the Web Start client runs outside of a browser, bookmarking, which is a browser feature, is disabled. Administrators can create Web Start clients that give users the same look as running an embedded bookmarked session. Set the following options in Deployment Wizard:

- Configure session:
  - Choose **yes** for Start Automatically.
  - Choose **no** for Start in Separate Window.



Start Options

Lock

Session ID: Automatic □

Start Automatically: ● Yes ○ No □

Start in Separate Window: ○ Yes ● No □

Auto-Start Options

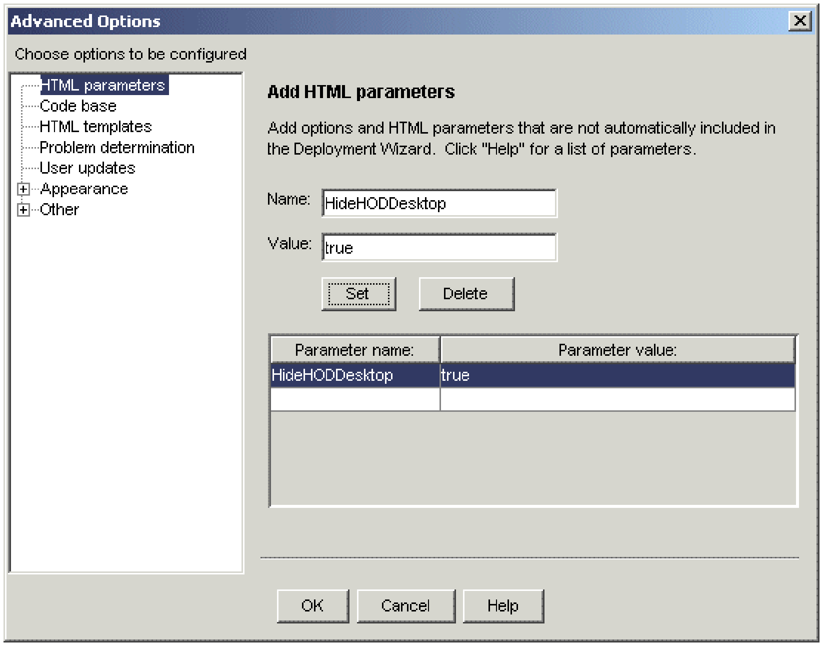
Applet/Macro: None □

Name: □

Parameter (Optional): □

Figure 16-18   Configuring bookmark-like Web Start client

- On the Advanced Options window of the Deployment Wizard, add the following parameter and value:
  – Parameter: HideHODDesktop
  – Value: true



Add HTML parameters

Add options and HTML parameters that are not automatically included in the Deployment Wizard. Click "Help" for a list of parameters.

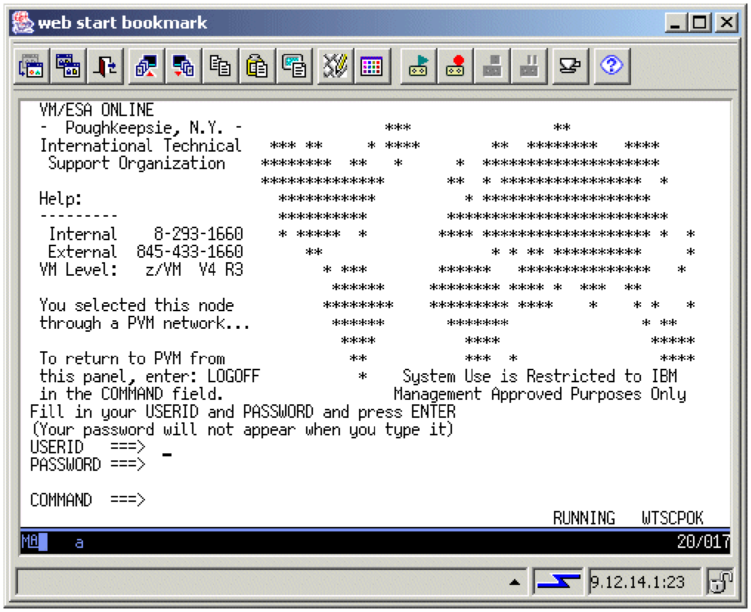
Name: HideHODDesktop

Value: true

Parameter name:	Parameter value:
HideHODDesktop	true

Figure 16-19   Configuring bookmark-like Web Start client

When the user starts the session, it will look something like what is shown in Figure 16-20.



```
 VM/ESA ONLINE
 -  Poughkeepsie, N.Y. -                ***                **
 International Technical   *** **     * ****        **  ********   ****
  Support Organization    ********  **   *      *  ********************
                          **************       **   * ****************  *
 Help:                      ***********           * *******************
 ---------                  **********         *************************
  Internal    8-293-1660    * *****  *        **** ******************* *  *
  External  845-433-1660       **                   * * ** **********      *
 VM Level:   z/VM  V4 R3         * ***        ******   ***************   *
                                  ******     ******** **** *  ***  **
 You selected this node          ********    ********* ****     *    * *  *
 through a PVM network...         ******       *******                * **
                                   ****          ****                 *****
 To return to PVM from              **           ***  *                ****
 this panel, enter: LOGOFF           *    System Use is Restricted to IBM
 in the COMMAND field.                   Management Approved Purposes Only
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>
PASSWORD ===>

COMMAND  ===>
                                                           RUNNING   WTSCPOK
MA    a                                                                  20/017
```

Figure 16-20   Bookmark-like Web Start client

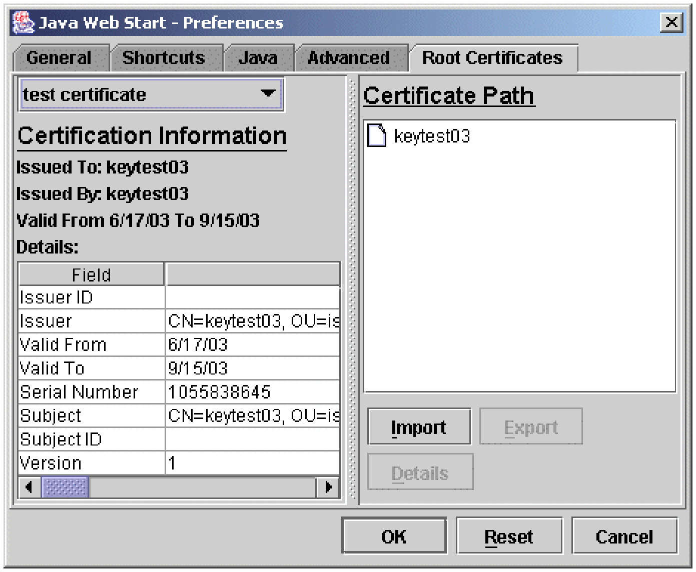
16.5.3 Using Web Start with HTTPS

If you want to use HTTPS with the Web Start client, the certificate authority used for your secure HTTP connection should come from a well-known root authority. Otherwise, you should import the signer certificate before establishing a connection.

When you use Host On-Demand as an applet and use an HTTPS connection, you are given the opportunity to trust the certificate used for the HTTPS connection if the root authority is not known by the browser. Since Java Web Start runs as an application, independently from a browser, you cannot use this browser function. The Java Virtual Machine used by Java Web Start contains several root authorities that it trusts. If the certificate that comes from the HTTPS connection has a root authority of one of these authorities known by the JVM, the secure connection can be established. If you want to use a certificate authority other than ones known by the JVM by default, for example, a self-signed certificate, you must import the certificate into the keystore of the JVM for each of the clients accessing this Java Web Start client. This is required to establish the secure HTTP connection.

To import certificate to the JVM keystore (procedure may varies with version/vendor of WSAM):

1. Start Java Web Start Application Manager.
2. Go to **File -> Preferences.**
3. Go to **Root Certificates tab.**
4. Click **Import** and select the certificate you want to import.



Certification Information

Issued To: keytest03

Issued By: keytest03

Valid From 6/17/03 To 9/15/03

Details:

Field	
Issuer ID	
Issuer	CN=keytest03, OU=is
Valid From	6/17/03
Valid To	9/15/03
Serial Number	1055838645
Subject	CN=keytest03, OU=is
Subject ID	
Version	1

Figure 16-21 Root Certificates tab after importing self-signed certificate for JWS 1.2

16.5.4 Removing the Web Start client

To remove the Web Start client, complete all of the following steps:

1. Launch Java Web Start Application Manager. Select **View -> Downloaded Applications**.
2. In the Applications: window, highlight the application you want to remove, and select **Application -> Remove Application**.
3. Launch HODRemove.html in your browser to clean the cache.

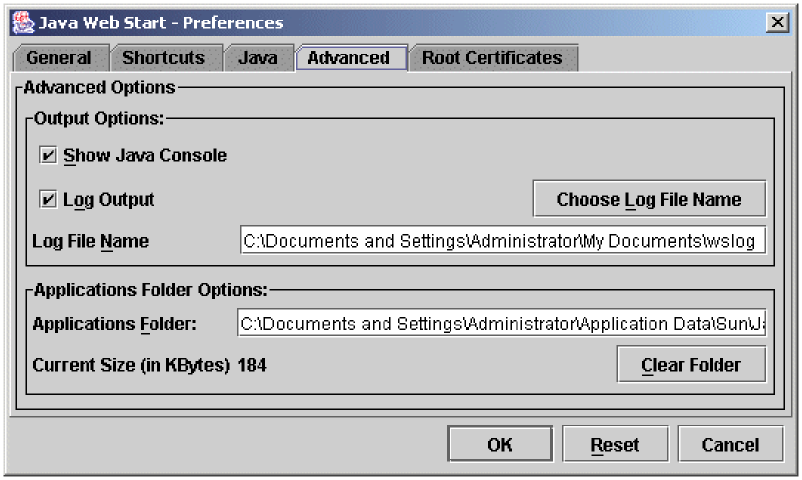
For Mac OS X, you will need to remove cache from the Java control panel. For instructions, refer to 5.5.2, “Remove cached client” on page 166.

16.5.5 Troubleshooting the Web Start client

In this section, we cover using the Java Console for Web Start clients.

Starting up the Web Start client

You can configure your client to show the Java Console from Java Web Start Application Manager. When setting this up, we recommend to turn on Log Output as well. See Figure 16-22.



☑ Show Java Console

☑ Log Output

Log File Name C:\Documents and Settings\Administrator\My Documents\wslog

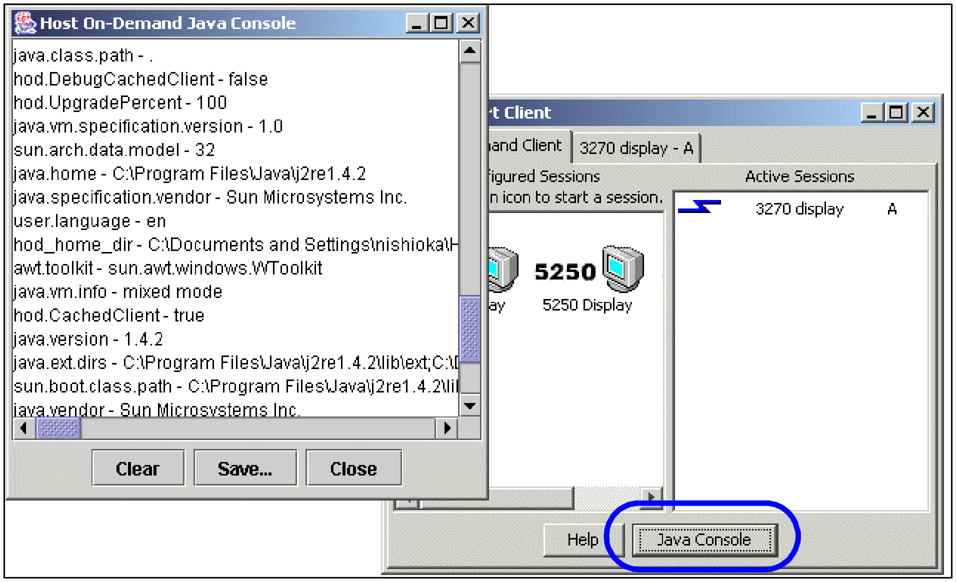
Applications Folder: C:\Documents and Settings\Administrator\Application Data\Sun\J

Current Size (in KBytes) 184

Figure 16-22 Setting to show Java Console for Java Web Start

While using Web Start client

Since there is no built-in Java Console for the Web Start client, you should use the custom Java Console which Host On-Demand provides. You can access it by clicking the **Java Console** button on the Host On-Demand desktop. With this Java Console, you can only dump the system properties by typing `s`.



```
java.class.path - .
hod.DebugCachedClient - false
hod.UpgradePercent - 100
java.vm.specification.version - 1.0
sun.arch.data.model - 32
java.home - C:\Program Files\Java\j2re1.4.2
java.specification.vendor - Sun Microsystems Inc.
user.language - en
hod_home_dir - C:\Documents and Settings\nishioka\H
awt.toolkit - sun.awt.windows.WToolkit
java.vm.info - mixed mode
hod.CachedClient - true
java.version - 1.4.2
java.ext.dirs - C:\Program Files\Java\j2re1.4.2\lib\ext;C:\I
sun.boot.class.path - C:\Program Files\Java\j2re1.4.2\lil
java.vendor - Sun Microsystems Inc.
```

Figure 16-23 Example of Web Start Java Console

Note: These two Java Console we discuss here are separate objects. Therefore, when troubleshooting the initial startup of a Web Start client, where you have to deal with Java Web Start Application Manager, you will need the Java Console set up by the Java Web Start Application Manager.

On the other hand, when you want to troubleshoot while a session is running, you will need the Custom-made Java Console provided by Host On-Demand, which you can launch from the Host On-Demand desktop.

16.6 More information for Web Start client

In this section, we provide information on files involved in the Web Start client.

16.6.1 HTML file for Web Start

The HTML file for Web Start client is shown in Example 16-1. When you access this HTML file, you will be directed to the corresponding JNLP file immediately.

Example 16-1 HTML file for Web Start

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<!-- HOD WIZARD HTML -->
<!-- Deployment Wizard Build : 8.0.0-B20030710 -->
```

```
<HTML>
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<TITLE>Web Start client</TITLE>
</HEAD>
<BODY BACKGROUND="hodbkgnd.gif">
<CENTER>
<IMG src="hodlogo.gif" ALT="hodlogo.gif">
<P>
<SCRIPT language="JavaScript">
window.onload = redirect ;
function redirect() {
top.location.href="WSclient.jnlp"
}
</SCRIPT>
</CENTER>
</BODY>
</HTML>
```

16.6.2 Java Network Launch Protocol (JNLP) file

The JNLP file generated by the Deployment Wizard is shown in Example 16-2. Note that the code base and minimum Java version are stated in this file.

Example 16-2 Example of JNLP file

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Deployment Wizard Build : 8.0.0-B20030710 -->
<jnlp codebase="http://ka0knhh/hod/" href="WSclient.jnlp">
  <information>
    <title>Web Start client</title>
    <vendor>IBM Corporation</vendor>
    <description>Web Start client</description>
    <offline-allowed/>
  </information>
  <security>
    <all-permissions/>
  </security>
  <resources>
    <j2se version="1.3+"/>
    <jar href="WSCachedSupporter2.jar" download="eager" main="true"/>
    <jar href="CachedAppletInstaller2.jar" download="eager"/>
    <property name="hod.WSFrameTitle"
value="Web%SPACECHAR%Start%SPACECHAR%client"/>
    <property name="hod.DocumentBase"
value="http://ka0knhh/hod/WSclient.jnlp"/>
```

```
    <property name="hod.PreloadComponentList"
value="HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HAMACRT;HACLTAU;HODHLL;HAVT;H
ASLP;HAKEYPD;HA3270;HAMACUI;HAPRINT;HODMAC;HALUM;HA3270X;HODCFG;SCCBASE;HA5250X
;HODSSL;HA3270P;HODTLBR;HASSL;HACICS;HAFTP;HASSH;HA5250P;HODZP;HAHOSTG;HAPD3270
;HAXFER;HA5250;HODAPPL;HAKEYMP;HACOLOR;HODIMP;HA5250E"/>
    <property name="hod.DebugComponents" value="false"/>
    <property name="hod.DebugCachedClient" value="false"/>
    <property name="hod.UpgradePromptResponse" value="Prompt"/>
    <property name="hod.UpgradePercent" value="100"/>
    <property name="hod.InstallerFrameWidth" value="550"/>
    <property name="hod.InstallerFrameHeight" value="250"/>
    <property name="hod.ParameterFile" value="HODData\WSclient\params.txt"/>
    <property name="hod.CachedClientSupportedApplet"
value="com.ibm.eNetwork.HOD.HostOnDemand"/>
    <property name="hod.CachedClient" value="true"/>
  </resources>
  <application-desc
main-class="com.ibm.eNetwork.HOD.cached.wssupport.WSCachedSupporter"/>
</jnlp>
```

For more information on the JNLP file and its tag, refer to the *Java Web Start Developer's Guide* at :

http://java.sun.com/products/javawebstart/docs/developersguide.html

17

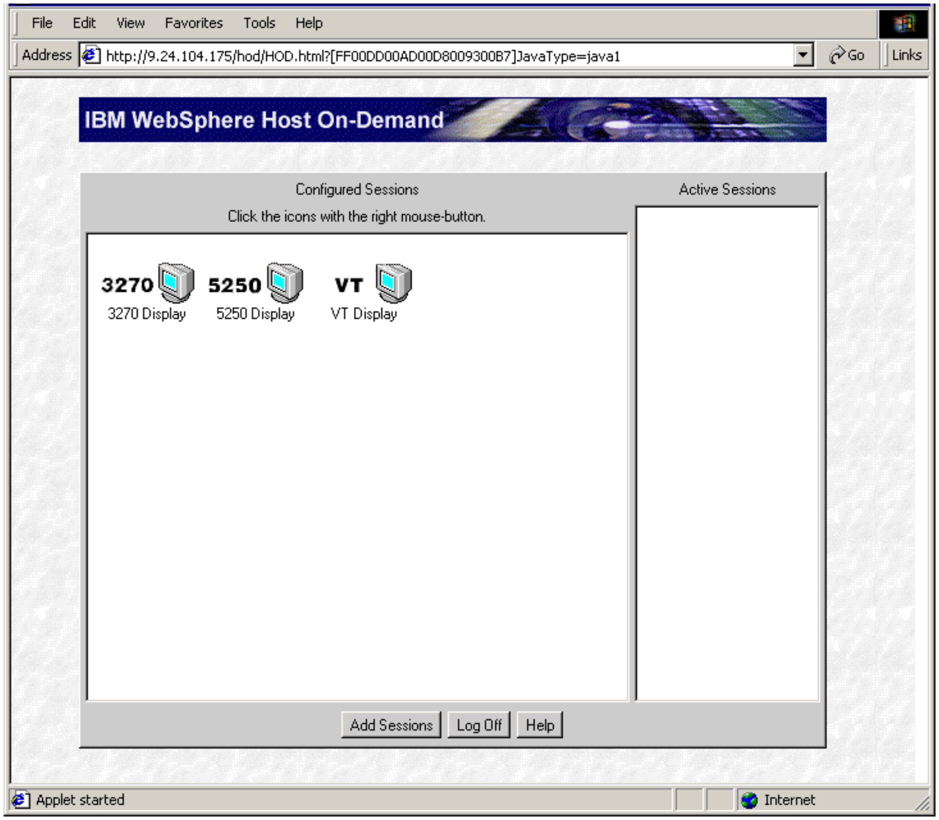
Custom HTML templates

In this chapter, we cover the support added in Host On-Demand to preserve customizations you make to a Host On-Demand Web page generated by the Deployment Wizard. This feature allows you to place the customizations in a separate file so that they are not lost if the Deployment Wizard is again used later on to modify the page.

17.1 Purpose of this feature

A custom HTML template is a file in which you can preserve HTML elements that modify the main HTML output file of the Deployment Wizard.

As you know, Deployment Wizard creates several output files (refer to 14.5, “Files created by the Deployment Wizard” on page 548). The main HTML output file is the file that contains the HTML and JavaScript elements that display the visible features of the Host On-Demand desktop page, shown in Figure 17-1.



Address http://9.24.104.175/hod/HOD.html?[FF00DD00AD00D8009300B7]JavaType=java1

Applet started

Figure 17-1 Default Host On-Demand desktop

Figure 17-1 shows the default Host On-Demand Desktop page with its light-gray textured background, with its IBM WebSphere Host On-Demand banner at the top, and its centrally located Host On-Demand desktop window containing the icons of configured sessions.

You might want to modify the main HTML output file of the Deployment Wizard in order to change the appearance of the Host On-Demand desktop page (for example, by replacing the Host On-Demand banner with a banner displaying your company's name); or to add HTML elements such as hyperlinks and forms to the page; or to add programming elements such as JavaScript or JavaServer Page elements.

Before Host On-Demand V7.0, you could make such changes by following these steps:

1. Running the Deployment Wizard to create output files
2. Manually editing the main HTML output file of the Deployment Wizard to add HTML elements, JavaScript elements, or JavaServer Pages elements

But there was a problem with this method. If later on for any reason you were to run the Deployment Wizard again to modify the main HTML output file (for example, in order to add an additional 3270 session), then the customized changes that you had added to the main HTML output file would be lost.

Specifically, the Deployment Wizard created a new main HTML output file that did not contain your customizations. You had to manually edit the new main HTML output file to add your customizations, just as you did the first time.

The custom HTML template feature alleviates this problem by allowing you to place your HTML, JavaScript, and JavaServer Pages' customizations in a separate file where they can be preserved. In order to work properly, the custom HTML template file must be based on a skeleton of text markers and basic HTML elements, which are defined in the file `Wizard.html` in the Host On-Demand publish directory.

The file `Wizard.html` also serves another purpose: if the user does not specify a custom HTML template file, Deployment Wizard uses the contents of `Wizard.html` as the skeleton for the main HTML output file.

Note: The Host On-Demand logon page is also affected.

The customizations in a custom HTML template file will affect not only the Host On-Demand desktop page, but also the accompanying Host On-Demand logon page, if your configuration model and options cause this page to be displayed.

17.1.1 Supported configuration models

You can use a custom HTML template file with any of the three Deployment Wizard configuration models:

- HTML-based model
- Configuration-server-based model
- Combined model

17.1.2 Client Java Types

You can use a custom HTML template file with any of the three Deployment Wizard Client Java Types:

- Java 1
- Java 2
- Autodetect

17.2 Name of the main HTML output file

The name of the main HTML output file created by Deployment Wizard is an implementation-specific detail that may change in later releases. However, in order to enable you to verify or debug elements that you have included in a custom HTML template, here is some information about the name of the main HTML output file in Host On-Demand Version 8.0.

The information is simple.

Table 17-1 Main HTML output file name

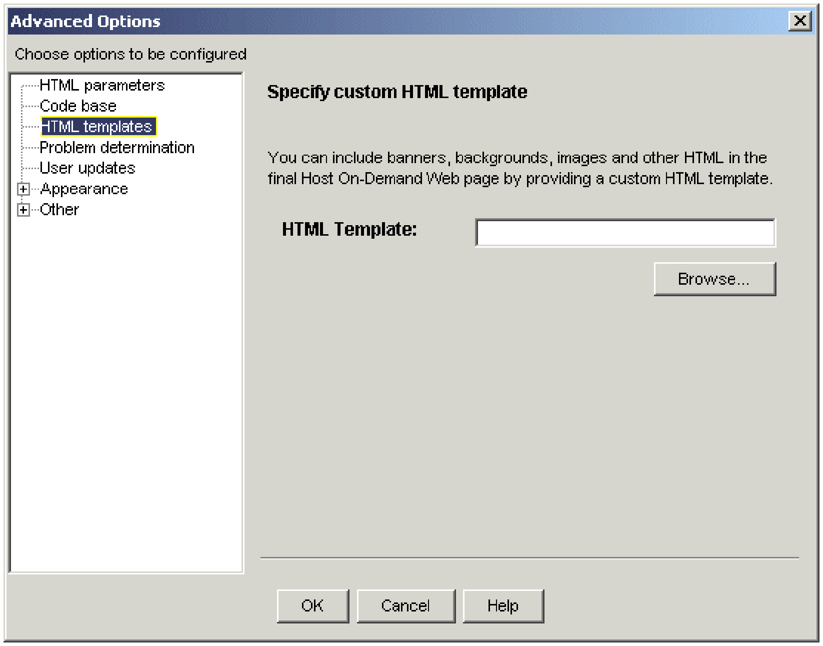
On the last page of the Deployment Wizard, in the File Name field, if you specify MyCompany	The name of the main HTML output file is
If the Client Java Type is Java 1	MyCompany.html
If the Client Java Type is Java 2 or Autodetect	z_MyCompany.html

17.3 Specifying a custom HTML template file

This section deals with specifying a custom HTML template file in the Deployment Wizard. For the basic information on this topic, see the Host On-Demand online documentation.

17.3.1 File management

To specify a custom HTML template in the Deployment Wizard, go to the Additional Options page, click **Advanced Options...**, then click **HTML templates**. Enter the file name in the HTML template field. (If you need a more detailed description of how to perform these steps, consult the section on the Deployment Wizard in the Host On-Demand online help.) Figure 17-2 shows the Advanced Options window with the HTML template field.



You can include banners, backgrounds, images and other HTML in the final Host On-Demand Web page by providing a custom HTML template.

HTML Template:

Figure 17-2 Advanced Options window, HTML templates selection

You can enter a file name, a relative path, or an absolute path. If you enter a file name or a relative path then Deployment Wizard starts looking for the file in the Host On-Demand publish directory.

It is probably better practice to enter an absolute path and maintain your custom template files in a separate directory outside of the Host On-Demand directory structure. This helps you keep custom HTML template files safe and separate from Deployment Wizard HTML output files.

You might want to identify all custom HTML template files by giving them a unique file extension or sequence of characters in the file name, for example, MyCompany.ctp or tplMyCompany.html.

17.3.2 Do not modify Wizard.html

You can modify Wizard.html directly instead of specifying a custom HTML template, but this is not a good idea. Instead, copy the contents of Wizard.html to a target file such as mytemplate.html, and modify the target file.

In fact, you should make a backup copy of Wizard.html in case you happen to yield to the temptation of taking a shortcut by modifying Wizard.html directly, or in case Wizard.html is corrupted accidentally.

Tip: Keep Wizard.html in pristine condition so that you can use it as a template for your custom HTML template files, and so that it can continue to be used as the default template when no custom template is specified.

If you do modify Wizard.html directly, do not specify a custom HTML template in the Deployment Wizard when you create the output files.

17.3.3 Custom HTML template versus Deployment Wizard output file

The main Deployment Wizard output file is the file whose name you specify in the File Name field on the File Name and Output Format page of the Deployment Wizard.

You also specify a main Deployment Wizard output file in the File Name: field on the Edit Existing HTML file page when you are starting out in the Deployment Wizard. On this page do not get confused and enter the name of a custom HTML template file. If you have associated a custom HTML template file with this main output file previously, the Deployment Wizard will look in the main output file and find the name of the custom HTML template file.

17.3.4 When error checking is performed

Deployment Wizard does not search for the custom HTML template file or inspect its contents until you click the **Create File(s)** button on the File Name and Output Format page. Therefore, Deployment Wizard will not inform you of any errors in the custom HTML template file until this point.

Here are some of the errors you might encounter:

- Deployment Wizard cannot find the custom HTML template, based on the path you specified.
- The custom HTML template file is not in valid UTF-8 format.
- The text markers in the custom HTML template file have been corrupted.

17.4 UTF-8 encoding

Your custom HTML template file should be in UTF-8 format, a standard format for storing Unicode characters. `Wizard.html` is in UTF-8 format. UTF-8 uses a unique sequence of 1, 2, 3, or 4 bytes to encode each character in the Unicode character set. Therefore, UTF-8 can handle all the Unicode characters, including all the characters of double-byte-character-set languages.

The Notepad editor included with Microsoft Windows 2000 and with Microsoft Windows XP is UTF-8 capable (but the Notepad editor included with Windows NT is not). When Notepad's Save As message box comes up, click the **Encoding:** combo box and select **UTF-8**.

If the UTF-8 formatting of a custom HTML template file becomes corrupted, then Deployment Editor will refuse to process the file.

17.4.1 Using an ASCII editor instead of a UTF-8 editor

Do not use an ordinary ASCII editor (one without the capability to save text in UTF-8 format) to save your custom HTML template file.

You can get by with using an ASCII-only editor if you use only characters in the lower-127-character range of the ASCII table, which includes English lowercase and uppercase letters, numbers, and many punctuation symbols. This approach works because for these characters UTF-8 uses the same 1-byte encodings as ASCII does. However, if you use any character in the upper-129-character range of the ASCII table (these are 1-byte ASCII characters that UTF-8 uses two or more bytes to encode), then Deployment Wizard may not be able to process the custom HTML template file, or may process it differently than you expect.

Given the risk of you accidentally introducing a character in the upper-129-character ASCII range, as well as for other reasons, you should not use an ASCII-only editor. Instead use a UTF-8 capable editor.

Two related points:

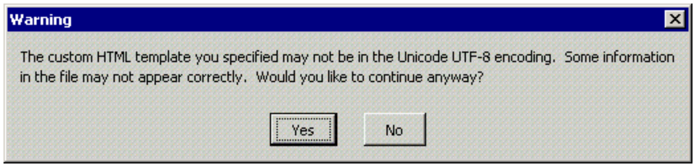
- 3-byte UTF-8 file signature

  If you use an ASCII-only editor to view a UTF-8 formatted file such as `Wizard.html` you will see the three characters *ï»¿* at the beginning of the file listing. These are the ASCII representation of a three-byte signature indicating to a UTF-8-capable editor that the file is in UTF-8 format. Do *not* delete these characters!

- UTF-8 warning message box

  The following information is implementation dependent and may change in future releases.

  You may see a message box warning you that your custom HTML template file may not be in UTF-8 format. This message box appears when the 3-byte UTF-8 file signature expected at the beginning of the file is missing. See Figure 17-3.



The custom HTML template you specified may not be in the Unicode UTF-8 encoding. Some information in the file may not appear correctly. Would you like to continue anyway?

Figure 17-3 Warning message about format of custom HTML template file

  This message box allows you to tell Deployment Wizard to continue and process the file anyway. However, when Deployment Wizard attempts to process the file, it will still expect the contents of the file to be encoded in UTF-8 format.

17.5 Parts of the custom HTML template file

This section discusses the different parts of a default custom HTML template file, and the significance of each part. In this section JavaServer Pages is abbreviated as JSP.

17.5.1 Default custom HTML template file

The following example shows a default custom HTML template file, which has exactly the same contents as `Wizard.html`.

Example 17-1 Contents of a default custom HTML template file

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<!-- SUMMARY -->
</HEAD>

<BODY BACKGROUND="<DW_CODE_BASE>hodbkgnd.gif">
<CENTER>
<IMG src="<DW_CODE_BASE>hodlogo.gif" ALT="hodlogo.gif">
<P>
```

```
<!-- STARTAPPLETPARMS -->
<!-- ENDAPPLETPARMS -->

<!-- SCRIPTS -->
<!-- APPLET -->

</CENTER>
</BODY>
</HTML>
```

17.5.2 Text markers

Do not delete or modify the text markers. Deployment Wizard uses these markers to indicate where certain types of information must be included in the main HTML output file.

The text markers are:

```
<!-- SUMMARY -->
<!-- STARTAPPLETPARMS -->
<!-- ENDAPPLETPARMS -->
<!-- SCRIPTS -->
<!-- APPLET -->
```

17.5.3 DOCTYPE declaration

The DOCTYPE declaration provides HTML version information and other information about the subsequent <HTML> element. Usually you will not need to modify this declaration.

The DOCTYPE declaration is copied to the main HTML output file without modification. Therefore any changes you make in this declaration in the custom HTML template file will be reflected in the main HTML output file.

Adding JavaScript and JSP after the DOCTYPE declaration

You can add JSP and JavaScript statements after the DOCTYPE declaration. The following example shows an unmodified DOCTYPE declaration followed by a JSP block. This is one of the JSP blocks used in an example of overriding HTML parameters in *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301.

The JSP block below includes JSP method calls, JavaScript statements, and Session Manager JavaScript API method calls.

Example 17-2 A JSP block added after the DOCTYPE declaration

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<%
//  Get a session or create one if necessary and store the hostname
//   entered in the form into the session.
HttpSession session = request.getSession(true);
String hostname = request.getParameter("form.hostname");

if (hostname!=null) {
    session.putValue("session.hostname", hostname);
}
%>
```

17.5.4 HEAD element

You can include HTML elements, JavaScript elements, and JSP elements within the HEAD element. Consult an HTML reference work to determine which HTML elements are valid within this element.

Place all the elements that you add to the HEAD element ahead of the `<!-- SUMMARY -->` marker. This is a suggestion for ease of use.

Information about particular elements or markers:

- TITLE

  Do not include a TITLE element. Deployment Wizard will generate a TITLE element in the main HTML output file using the text you enter in the Page Title: field of the File Name and Output Format page.

- META

  You can modify the META element in the default custom HTML template file. This element is copied to the main HTML output file without modification.

  You can add additional META elements.

- `<!-- SUMMARY -->`

  This marker indicates where Deployment Wizard will include in the main HTML output file a lengthy HTML comment summarizing the options selected in the Deployment Wizard pages.

Example 17-3 shows a HEAD element with changes. Note that:

- The original META element has not been modified, even though it could have been.
- A new JavaScript element contains a method called calculateCelsius().
- Two additional META elements specify author and copyright information.

- All the changes have been included before the `<!-- SUMMARY -->` marker.

Example 17-3 Example modifications to HEAD element

```
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<SCRIPT LANGUAGE="JAVASCRIPT">
function calculateCelsius(theForm)
{
   var fahrenheit = parseFloat(theForm.fahrenheitText.value);
   theForm.celsiusText.value = (5.0/9.0 * (fahrenheit - 32.0)).toString();
}
</SCRIPT>
<META NAME=author  CONTENT="John Smith">
<META NAME=copyright CONTENT="Copyright 2002, My Company">
<!-- SUMMARY -->
</HEAD>
```

17.5.5 BODY element

You can include HTML elements, JavaScript elements, and JSP elements within the BODY element. Consult an HTML reference work to determine which HTML elements are valid within this element.

You can modify the attributes of the BODY element itself. For example, you might want to specify a different image for the background or a solid background color instead of an image.

In the default custom HTML template file the `<DW_CODE_BASE>` variable in the BACKGROUND attribute indicates that the file is located in the `images` subdirectory of the Host On-Demand publish directory. See Example 17-1 on page 622.

17.5.6 Within BODY before <!-- STARTAPPLETPARMS -->

Placement

Elements in this section will be placed in the main HTML output file ahead of the APPLET element that launches the Host On-Demand applet. Consequently, displayable elements in this section will be displayed on the Host On-Demand desktop page ahead of the Host On-Demand desktop window.

CENTER, IMG, P

In the default custom HTML template file (see Example 17-1 on page 622) the following lines appear after the line containing the `<BODY>` tag as shown in Example 17-4.

Example 17-4 Three lines following the line containing the <BODY> tag

```
<CENTER>
<IMG src="<DW_CODE_BASE>hodlogo.gif" ALT="hodlogo.gif">
<P>
```

In connection with these lines, please note:

- IMG

  You can delete or modify this element.

- CENTER

  Remember that the `<CENTER>` tag requires a `</CENTER>` closing tag later in the file. In the default custom HTML template file, the `</CENTER>` closing tag occurs on the third line from the bottom of the file.

  You will probably want to retain this element. In a default HTML template file this element causes the Host On-Demand desktop window to be displayed centered in the browser page.

- P

  You will probably want to retain this element or something like it. In a default HTML template file, this element prevents the IBM WebSphere Host On-Demand banner from being displayed on the same line as the Host On-Demand desktop window.

Example

Example 17-5 notes that:

- The BODY element has been modified to specify non-default colors for background, text, and links.
- The IMG element has been deleted.
- An H1 element is used to display the company name, MyCompany, Inc.
- The CENTER element is retained, so that the link and the Host On-Demand desktop will be centered.
- An A element is used to display a link to the company home page.
- The P element is retained, so that the Host On-Demand desktop will be displayed below the link element instead of on the same line.

Example 17-5 Sample section before <!-- STARTAPPLETPARMS -->

```
<BODY BGCOLOR="GRAY" TEXT="WHITE" VLINK="WHITE" LINK="LIME" ALINK="YELLOW">
<h1 align=center><i><font size=7 face="Impact" color="WHITE">MyCompany,
Inc.</font></i></h1>
<CENTER>
<A HREF="http://www.mycompanyinc.com">MyCompany Home Page</A>
<P>

<!-- STARTAPPLETPARMS -->
```

The changes in the above example added to a default custom HTML template file create the following customized browser page in Figure 17-4.

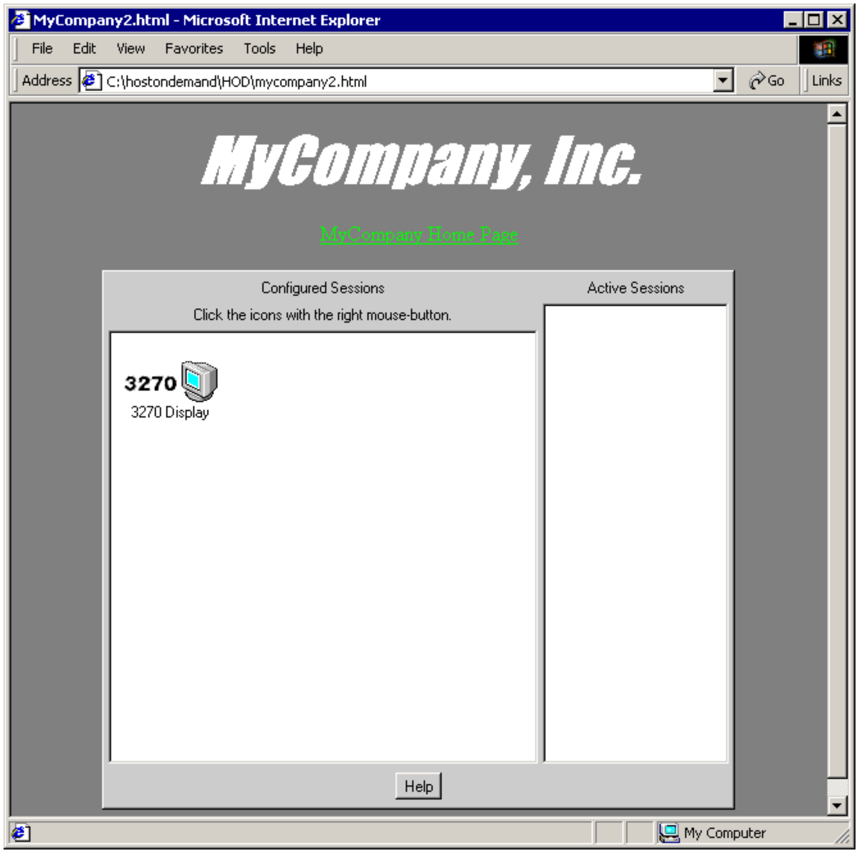


Figure 17-4 Customized browser page with <h1> heading and link

17.5.7 Within BODY between <!-- STARTAPPLETPARMS --> and <!-- ENDAPPLETPARMS -->

This section should be used only to specify session parameters. Do not specify session parameters anywhere else in the custom HTML template file

The session parameters are documented in the Host On-Demand online help, and include the following types of parameters:

- Session1 parameters
- Session2 parameters
- 3270 and 5250 host print parameters
- The Disable parameter
- Cached client parameters
- The "additional parameters" in Deployment Wizard (such as CustomKeyFunctionX and DoNotPrefillUser)
- The TraceOptions parameter
- The IPMonitor parameter

To specify a session parameter, use the format <PARAM NAME=*name* VALUE=*value*>. The following example shows a `Disable` parameter and an `IgnoreWellKnownTrustedCAs` parameter.

Example 17-6 Sample section specifying session parameters

```
<!-- STARTAPPLETPARMS -->
<PARAM NAME="Disable"    VALUE="cutpaste;filexfer3207;filexfer5250">
<PARAM NAME="IgnoreWellKnownTrustedCAs" VALUE="true">
<!-- ENDAPPLETPARMS -->
```

17.5.8 Within BODY between <!-- ENDAPPLETPARMS --> and <!-- APPLET -->

Do not add anything here. Specifically, do not add any elements between `<-- ENDAPPLETPARMS -->` and `<-- SCRIPTS-->`, and do not add any elements between `<!--SCRIPTS -->` and `<!-- APPLET -->`.

The `<!-- SCRIPT -->` marker indicates where Deployment Wizard will add required JavaScript code. Do not put your custom JavaScript code here.

The `<!-- APPLET -->` marker indicates where the Deployment Wizard will add the APPLET element used to launch the Host On-Demand applet.

In short, this section of your custom HTML template file should be the same as it is in the default HTML template file. Example 17-7 illustrates this.

Example 17-7 Sample section after <!-- ENDAPPLETPARMS -->

```
<!-- ENDAPPLETPARMS -->

<!-- SCRIPTS -->
<!-- APPLET -->
```

17.5.9 Within BODY after <!-- APPLET -->

Placement

Elements in this section will be placed in the main HTML output file after the APPLET element that launches the Host On-Demand applet. Consequently, displayable elements in this section will be displayed on the Host On-Demand desktop page after the Host On-Demand desktop window.

CENTER, P

If you do not have a `<CENTER>` tag in the section before `<!-- STARTAPPLETPARMS -->` then you do not need a closing `</CENTER>` tag in this section.

If you include a displayable element in this section, then you should put a P element ahead of it, so that the displayable element is displayed below the Host On-Demand desktop window instead of on the same line.

Example

In the following example note that:

- A FORM element has been added which displays check boxes, a **Clear** button, and a **Submit** button.
- The P element causes the FORM element to be displayed below the Host On-Demand desktop window instead of on the same line.

Example 17-8 Sample section after <!-- APPLET -->

```
<!-- APPLET -->
<P>
<FORM METHOD="POST" ACTION="someplace/foo.cgi"
ENCTYPE="application/x-www-form-urlencoded">
What additional applets would you like to run?<BR>
<INPUT TYPE="checkbox" NAME="choice"
            VALUE="TravelExp">MyCompany Travel Expenses<BR>
<INPUT TYPE="checkbox" NAME="choice"
            VALUE="CapEquip">MyCompany Capital Equipment<BR>
<INPUT TYPE="checkbox" NAME="choice"
```

```
            VALUE="PhoneLog">MyCompany Phone Log<BR>
<INPUT TYPE="reset" VALUE="Clear Form">
<INPUT TYPE="submit" VALUE="Submit">
</FORM>

</CENTER>
</BODY>
</HTML>
```

The changes in Example 17-8 added to a default custom HTML template file create the following customized browser page in Figure 17-5.

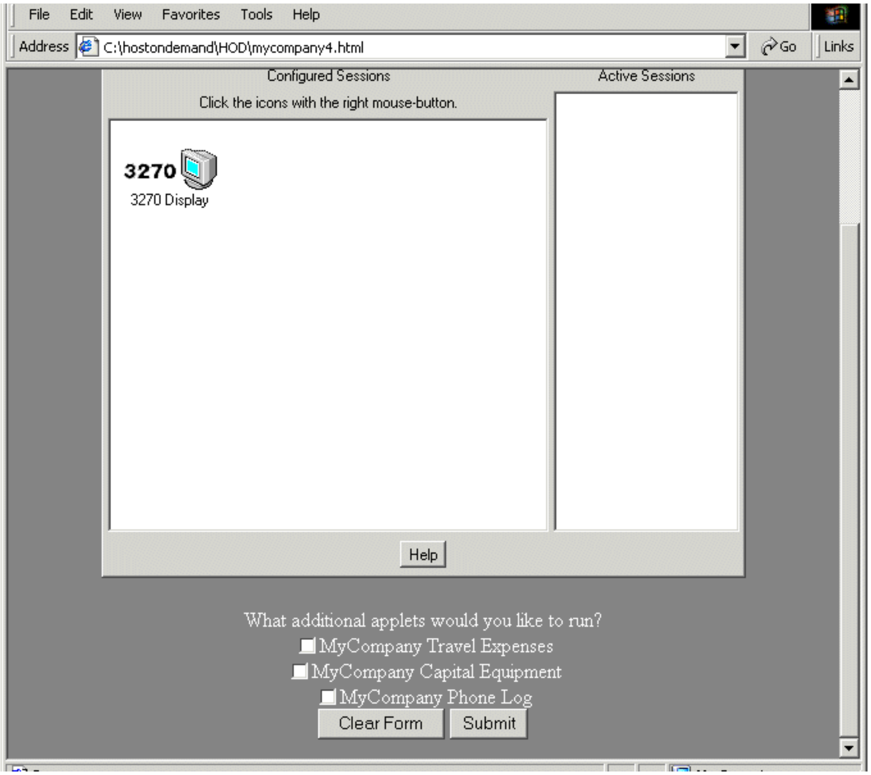

File
Edit
View
Favorites
Tools
Help
Address
C:\hostondemand\HOD\mycompany4.html
Go
Links
Configured Sessions
Active Sessions
Click the icons with the right mouse-button.
3270
3270 Display
Help
What additional applets would you like to run?
□ MyCompany Travel Expenses
□ MyCompany Capital Equipment
□ MyCompany Phone Log
Clear Form
Submit

Figure 17-5 Customized browser page with FORM

18

Modifying session properties dynamically (using HTML overrides)

Modifying session properties dynamically means overriding one or more fixed Host On-Demand session property values at the time client users access the HTML files. These session property values can be overridden based on information such as the client's IP address or the time of day. Administrators modify session properties dynamically by completing two main tasks:

- Modifying the HTML code that is generated from the Host On-Demand Deployment Wizard
- Deploying a program that runs on the Web server

You can override several session properties, including the LU (logical unit) name, the workstation ID of the client, the port, as well as the host name. For a complete list, refer to 18.3, "Session properties that can be overridden" on page 634.

In this chapter, we describe the benefits of modifying session properties dynamically, provide information that will help you decide if using this feature is more useful for your company, and give you step-by-step examples of two common real-life scenarios that can help you take advantage of this time-saving feature.

18.1 Benefits of modifying session properties dynamically

By allowing you to override session properties at the time users access Host On-Demand HTML files, you can redefine session properties without having to reconfigure the HTML files themselves. Since reconfiguring the HTML files can be very time consuming, this feature is attractive because it allows you to make changes in a fraction of the time normally associated with redefining session properties for users.

When you override session properties, the override values always take precedence over both the initial session properties that were defined by the administrator, as well as any user updates to the session properties. When the administrator decides to remove an override value for a session property, the initial configuration for the property becomes active again. This is because the HTML override value is never stored. This type of control allows you to make changes whenever necessary without losing your original settings. Also, the override value is locked, so the user cannot change it.

Administrators can choose from a variety of ways to modify session properties dynamically. Although it always involves modifying the HTML file that you create using the Deployment Wizard, you can write the program that runs on the Web server using a number of different programming languages, including JavaServer Pages (JSPs), servlets, Perl, REXX, or Active Server Pages (ASPs). Although this requires a basic understanding of Common Gateway Interface (CGI) applications, you do not have to be an expert in any of these programming languages. The two example scenarios that we provide in the following sections use JSPs.

18.2 The need to dynamically modify session properties

Although there are many reasons why administrators may want certain session properties to be overridden at the time users retrieve Host On-Demand sessions, the most common examples involve either overriding a certain property value, such as LU name based on the client's IP address, or providing a form in which the client can enter information, such as their host name or terminal size. In this chapter, we provide two real-life scenarios based on these common administrator issues, which may help you determine if your company should take advantage of this feature.

18.3 Session properties that can be overridden

Table 18-1 shows which session properties can be overridden, describes them, and provides acceptable values for each session property parameter.

Table 18-1 Session properties

Parameter name	Description	Valid values
Host	Host name or IP address of the target server. Appears as “Destination address” on property windows. Applies to all session types.	Host name or IP address.
Port	The port number on which the target server is listening. Appears as “Destination port” on property windows. Applies to all session types.	Any valid TCP/IP port number.
CodePage	The codepage of the server to which the session will connect. Appears as “Host Code-Page” on property windows. Applies to all session types except FTP.	The numeric portion (for example, 037) of the supported host codepage listed in the session property window.
SessionID	The short name you want to assign to this session (appears in the OIA). It must be unique to this configuration. Appears as “Session ID” on property windows. Applies to all session types.	One character: A-Z.
LUName	The name of the LU or LU Pool, defined at the target server, to which you want this session to connect. Appears as “LU or Pool Name” on property windows. Applies to 3270 Display and 3270 Printer session types.	The name of an LU or LU Pool.

Parameter name	Description	Valid values
WorkstationID	The name of this workstation. Appears as “Workstation ID” on property windows. Applies to 5250 Display and 5250 Print session types.	A unique name for this workstation.
ScreenSize	Defines the number of rows and columns on the screen. Appears as “Screen Size” on property windows. Applies to 3270 Display, 5250 Display, and VT Display session types.	value=rows x columns 2=24x80 (3270, 5250, VT) 3=32x80 (3270) 4=43x80 (3270) 5=27x132 (3270, 5250) 6=24x132 (VT) 7=36x80 (VT) 8=36x132 (VT) 9=48x80 (VT) 10=48x132 (VT) 11=72x80 (VT) 12=72x132 (VT) 13=144x80 (VT) 14=144x132 (VT) 15=25x80 (VT) 16=25x132 (VT)
SLPScope	Service Location Protocol (SLP) Scope. Appears as “Scope” under “SLP Options” on property windows. Applies to 3270 Display, 3270 Printer, 5250 Display, and 5250 Printer session types.	Contact your administrator to get the correct value for this field.
SLPAS400Name	Connects a session to a specific iSeries. Appears as “AS/400 Name (SLP)” on property windows. Applies to 5250 Display and 5250 Printer session types.	The fully qualified SNA CP name (for example, USIBMNM.RAS400B).

Parameter name	Description	Valid values
SSLCertificateSource	The certificate can be kept in the client's browser or dedicated security device, such as a smart card; or, it can be kept in a local or network-accessed file. Appears as “Certificate Source” on property windows. Applies to 3270 Display, 3270 Printer, 5250 Display, 5250 Printer, and VT Display session types.	The value is SSL_CERTIFICATE_IN_CSP for a certificate in a browser or security device. The value is SSL_CERTIFICATE_IN_URL for a certificate in a URL or file.
SSLCertificateURL	Specifies the default location of the client certificate. Appears as “URL or Path and Filename” in property windows. Applies to 3270 Display, 3270 Printer, 5250 Display, 5250 Printer, and VT Display session types.	The URL protocols you can use depend on the capabilities of your browser. Most browsers support HTTP, HTTPS, FTP, and FTPS.
FTPUser	Specifies the user ID the session uses when connecting to the FTP server. Appears as “User ID” on property windows. Applies to FTP session types.	A valid user ID.
FTPPassword	Specifies the password the session uses when connecting to the FTP server. Appears as “Password” on property windows. Applies to FTP session types.	A valid password.
UseFTPAnonymousLogon	Enables the session to log in to an FTP server using anonymous as the user ID. Appears as “Anonymous Login” on property windows. Applies to FTP session types.	Yes or No.

Parameter name	Description	Valid values
FTPEmailAddress	Specifies the e-mail address to use when connecting to the FTP server while using Anonymous Login. Appears as “E-mail Address” on property windows. Applies to FTP session types.	A valid e-mail address.
Netname	The name of the terminal resource to be installed or reserved. If this field is blank, the selected terminal type is not predictable. Applies to CICS sessions only.	A valid terminal resource name.

18.4 Scenario 1: Overriding the LU name based on client IP address

A company with over 1000 Host On-Demand clients prefers its users to have the same LU name every time they log on to their 3270 Display and Printer sessions to better allocate resources in their mainframe environment. However, the company’s administrator does not want to spend unnecessary time having to specify the LU names directly in the session definitions. Instead, he decides to modify the session properties dynamically so that the LU name is determined from the IP address of the client at the time users access the HTML file.

In this scenario, the administrator creates a text file called `luname.table` that pairs LU names with IP addresses, so that the proper LU names are assigned to the clients based on their corresponding IP addresses. He creates a JSP file that reads this text file into a properties variable.

In the following section, we provide the steps that this administrator takes to modify the session properties, including editing the HTML code and deploying a JSP on the Web server. Following the steps, we show you an example of the completed JSP code.

Note: The following instructions are specific for this company's environment, which includes a Windows 2000 operating system and IBM WebSphere Application Server Advanced Edition Version 4.0. Other environments may require different steps.

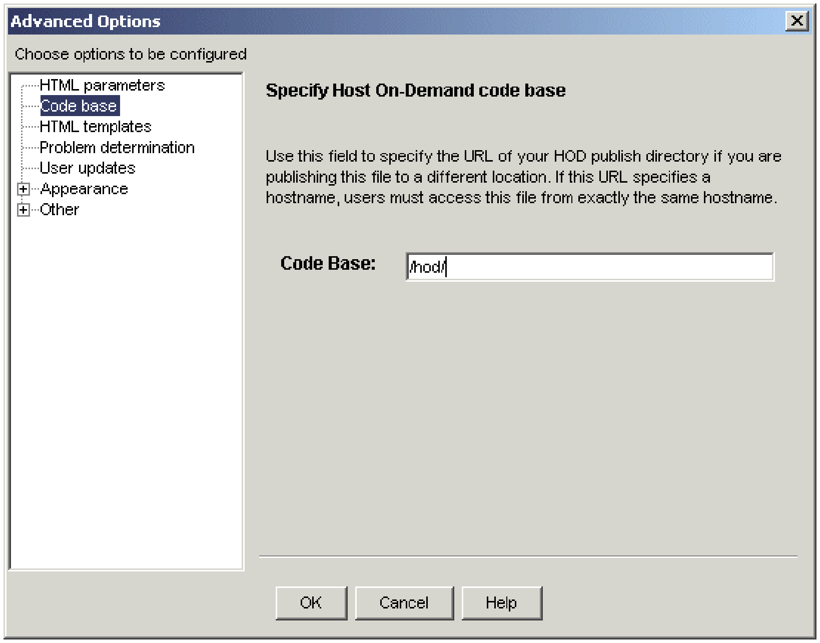
18.4.1 Steps to modify the session properties

Follow these steps in order to override the LU name based on the client's IP address:

1. Use the Deployment Wizard to set up your initial HTML file. On the Additional Options window, click **Advanced Options** and go to the **Other** tab. Type the relative path `/hod/` in the Codebase field (Figure 18-1). Save the HTML file to the default Host On-Demand publish directory `/HostOnDemand/HOD`. Your HTML file is now in the same directory with Host On-Demand's archive files.

Important: Codebase refers to the installed Host On-Demand publish directory, not the directory where you publish your Deployment Wizard files. Although you can enter a fully qualified URL in the Codebase field, we strongly recommend that you enter the relative path `/hod/` for the default publish directory when modifying session properties dynamically. If you enter a fully qualified URL, any users who specify the host name in a different manner than you specified as the Codebase will not be able to access the files, even if the DNS entries resolve to the same IP address.

For more information about Codebase and which files are created by the Deployment Wizard, refer to Chapter 14., "Deployment Wizard" on page 517.



Specify Host On-Demand code base

Use this field to specify the URL of your HOD publish directory if you are publishing this file to a different location. If this URL specifies a hostname, users must access this file from exactly the same hostname.

Code Base: /hod/

Figure 18-1 Codebase selection window of the Deployment Wizard

Note the following points:

– The Deployment Wizard generates some of the HTML code using JavaScript, and the HTML parameters are specified within a JavaScript array, or by means of JavaScript document.write statements.

– The format of the HTML code generated by the Deployment Wizard depends on whether you select **Java 1**, **Java 2**, or **Autodetect** for the Client Java Type, and whether or not you cache the Host On-Demand applet on your users' machines. Both of these options appear on the Additional Options window of the Deployment Wizard. (This scenario uses a cached Java 1 HTML file.)

2. Read a file called luname.table, which you will create in the next step into a properties variable by adding the following lines to your JSP code:

```
<%java.util.Properties lunames = new java.util.Properties();
   lunames.load(new java.io.FileInputStream(“c:\\luname.table”));%>
```

(This code assumes that the luname.table file is located on your C: drive.) See 1 on page 652 to see where these lines are located in the JSP code.

3. Create a file called luname.table file that contains pairs of LU names and IP addresses. The user's browser requests the IP address of the user, and the corresponding LU name is looked up from this luname.table file and read into

a properties variable that can be used by the JSP file. The format of the lines should be ipaddress=luname, for example, `9.33.67.5=luname`.

4. Enable HTML overrides by including the EnableHTMLOverrides parameter in your HTML file and setting it to a value of true, as in the following example:

   ```
   document.write('<PARAM NAME="EnableHTMLOverrides" VALUE="true">');
   ```

   Refer to 2 on page 654 to see where this line is located in the JSP code.

5. List the sessions to be overridden by including the TargetedSessionList parameter, and setting the value as the exact names of the sessions that you are modifying dynamically. Since you may have multiple sessions associated with your HTML file, you need to specify which sessions you are modifying.

   In the following example, the administrator set the value as the list of session (names 3270 Display and 5250 Display) and separated them with commas:

   ```
   document.write('<PARAM NAME="TargetedSessionList"
      VALUE="3270 Display,5250 Display">');
   ```

   Refer to 3 on page 654 to see where these lines are located in the JSP code.

6. Specify the override itself by including an HTML parameter for each of the properties that you are overriding. The name of the HTML parameter should be the name of the session property, and the value should be a value for the desired override.

   In this scenario, by inserting the following code, the administrator changed the LUName session parameter for the session called 3270 Display. The LU name is set to the LU name corresponding to the IP address in `c:\\luname.table`.

   ```
   document.write('<PARAM NAME="Luname" VALUE="3270
      Display=<%=lunames.get(request.getRemoteAddr())%>">');
   ```

   The request.getRemoteAddr() is Java code for getting the IP address of the client requesting the JSP. This IP address is used to look up the corresponding LU name in the variable containing the luname.table file.

   Refer to 4 on page 654 to see where these lines are located in the JSP code.

7. Add a ConfigBase parameter to the JSP file:

   ```
   document.write('<PARAM NAME="ConfigBase" Value="http://host_name/hod/">');
   ```

Important: Similar to defining `/hod/` as the Codebase in Step 1, the ConfigBase parameter is necessary because you will eventually deploy your JSP file to a location that is different than the default publish directory, and the Host On-Demand applet needs to know how to find the session configuration files located in the `HostOnDemand/HOD/HODData` directory. These files are created at the same time you save your Deployment Wizard HTML file to the publish directory.

Unlike Codebase, the ConfigBase parameter requires a fully qualified URL. ConfigBase is a term that is specific to Host On-Demand.

For more information, refer to 14.5, “Files created by the Deployment Wizard” on page 548.

Refer to 5 on page 654 to see where this line is located in the JSP code.

8. Compare your new JSP code to make sure that it is identical to the code in the file provided in 18.4.3, “Completed HTML file after edits” on page 652. If not, make the necessary changes. If so, change the file extension from HTML to JSP and save it to your machine.
9. Start the WebSphere Application Server Advanced Edition Version Application Assembly Tool by selecting **Start -> Programs -> IBM WebSphere -> Application Server V4.0 AE -> Application Assembly Tool**. The Application Assembly Tool helps you package your application according to the J2EE specifications.

In this scenario, since we are packaging a JSP file, we need to create a Web module using the Create Web Module Wizard (Figure 18-2). Highlight the wizard and click **OK**.

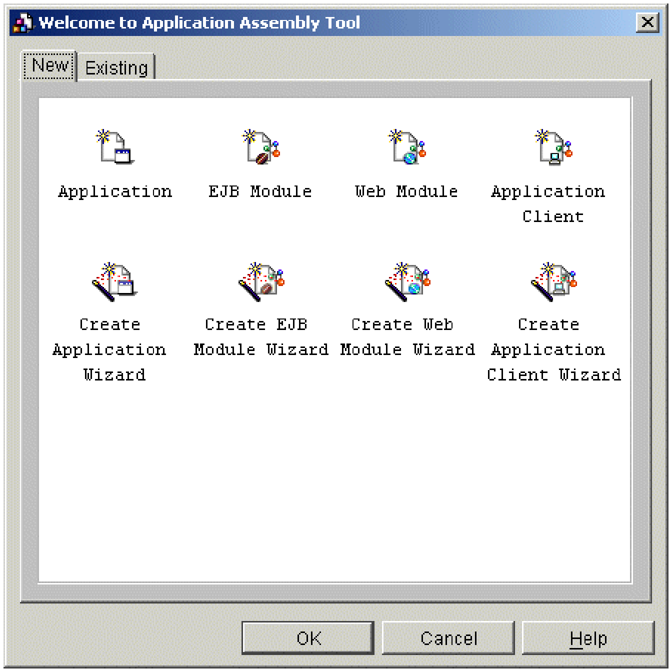
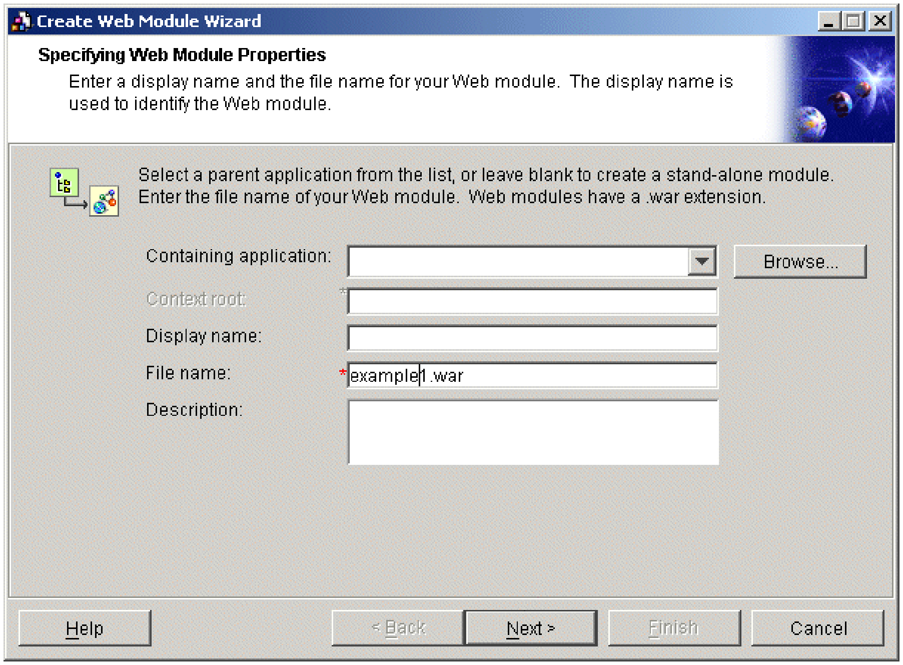


Figure 18-2 Application Assembly Tool

10. On the Specifying Web Module Properties window (Figure 18-3), type the name of your WAR (Web archive) file in the File name field. This WAR file represents your Web module. Although you will see the default name `Web_Name_Module1.war` in this field, you may want to change it to another name. Note that the File name field is the only field on this window that requires you to enter information (as indicated by the asterisk). Once you name your WAR file, click **Next**.



Specifying Web Module Properties

Enter a display name and the file name for your Web module. The display name is used to identify the Web module.

Select a parent application from the list, or leave blank to create a stand-alone module. Enter the file name of your Web module. Web modules have a .war extension.

Containing application:

Context root: *

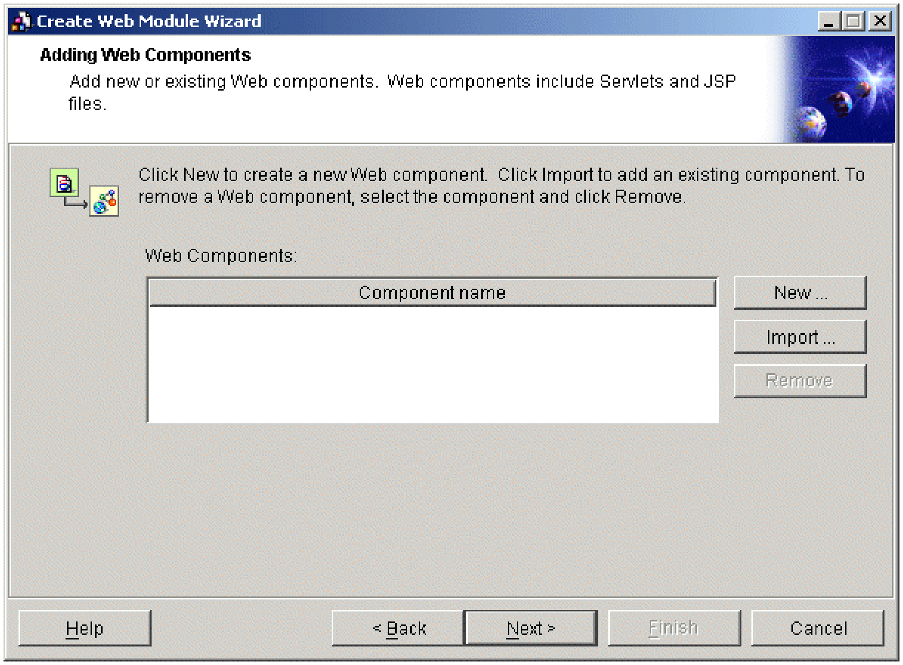
Display name:

File name: * example1.war

Description:

Figure 18-3 Specifying Web Module Properties

11. Click through four windows until you get to the Adding Web Components window, as shown in Figure 18-4. Click **New**. This launches a second wizard called Create Web Component Wizard. Now, you have two open wizards on your work space at the same time.



Adding Web Components

Add new or existing Web components. Web components include Servlets and JSP files.

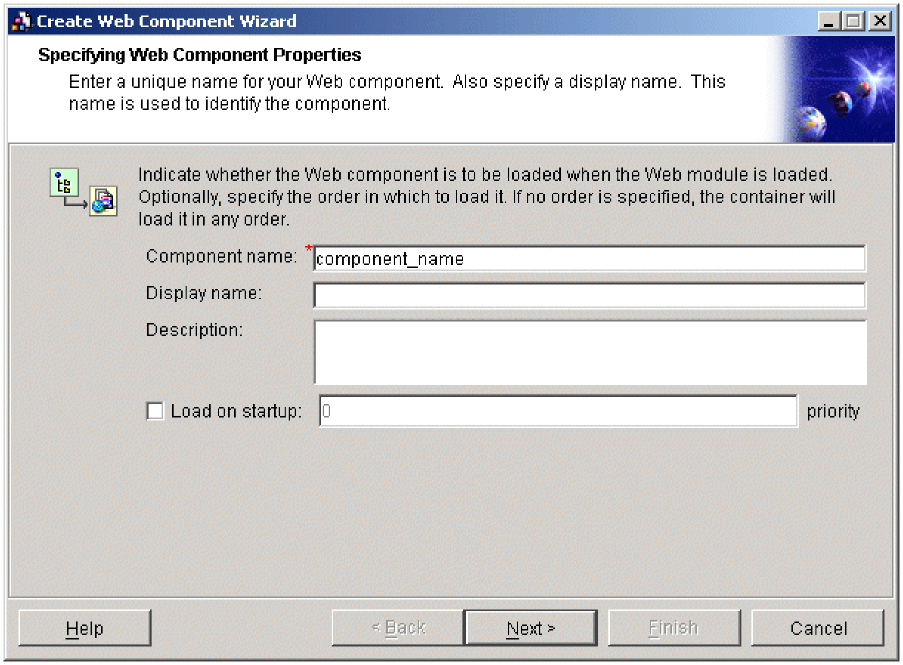
Click New to create a new Web component. Click Import to add an existing component. To remove a Web component, select the component and click Remove.

Web Components:

Component name

Figure 18-4 Adding Web Components

12. The first window of the Create Web Component Wizard is called Specifying Web Component Properties (Figure 18-5). In the Component name field, type the name of the Web component. The name of this component must be unique. You can also provide a display name and component description, but these fields are not required.



Create Web Component Wizard

Specifying Web Component Properties

Enter a unique name for your Web component. Also specify a display name. This name is used to identify the component.

Indicate whether the Web component is to be loaded when the Web module is loaded. Optionally, specify the order in which to load it. If no order is specified, the container will load it in any order.

Component name: * component_name

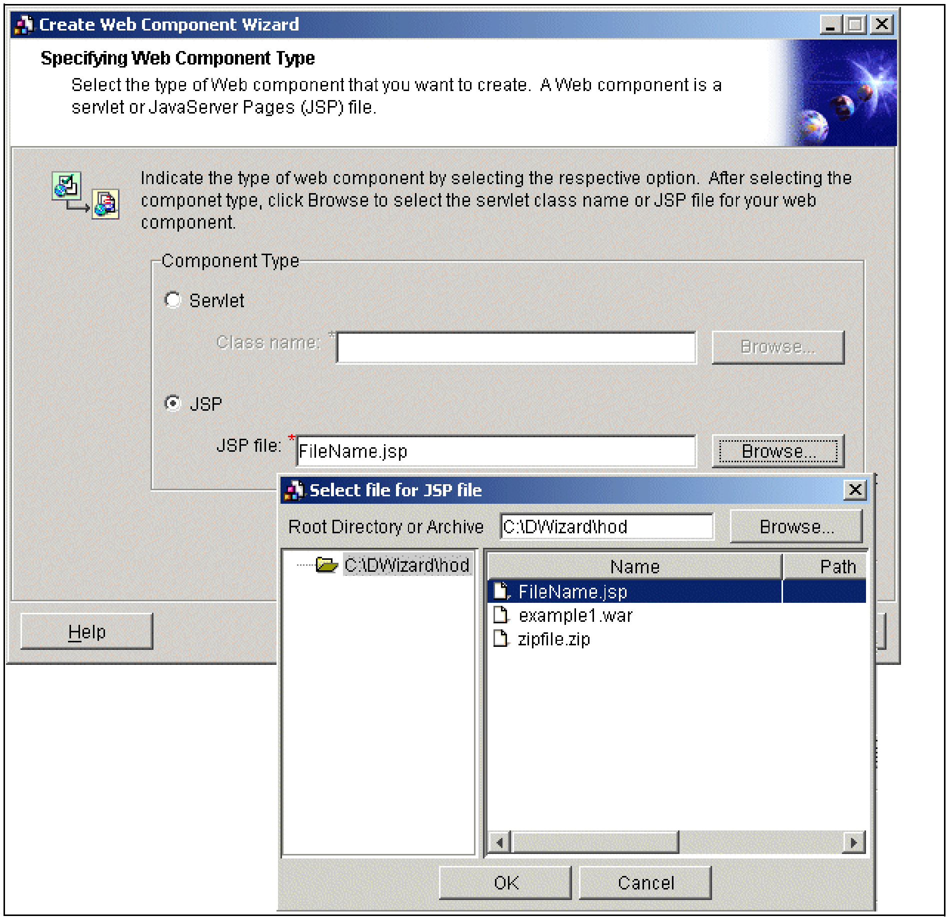
Display name:

Description:

□ Load on startup: 0 priority

Figure 18-5 Specifying Web Component Properties

13. On the Specifying Web Component Type window (Figure 18-6), select **JSP** and then click **Browse**. After the Select file for JSP file appears, click **Browse** to select the root directory of the JSP file that you created in step 8. on page 641. Once you find and highlight the root directory, click **Select.** The JSP file contained in the directory appears in the right frame of the window. Highlight the **JSP file** and click **OK**. After you click **OK**, the name of the JSP file appears in the JSP field in the wizard window.



Create Web Component Wizard

Specifying Web Component Type

Select the type of Web component that you want to create. A Web component is a servlet or JavaServer Pages (JSP) file.

Indicate the type of web component by selecting the respective option. After selecting the componet type, click Browse to select the servlet class name or JSP file for your web component.

Component Type

○ Servlet

Class name: *

● JSP

JSP file: * FileName.jsp

Select file for JSP file

Root Directory or Archive: C:\DWizard\hod

C:\DWizard\hod

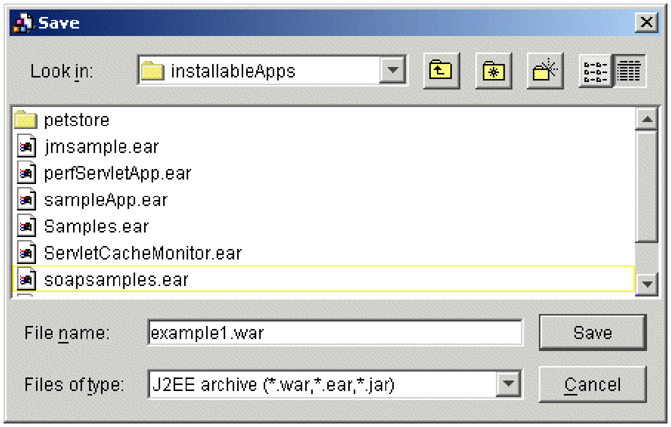
Name	Path
FileName.jsp	
example1.war	
zipfile.zip	

Figure 18-6 Specifying Web Component Type

14. Click **Next** until you reach the final window of the Create Web Component Wizard. Click **Finish**. Click **Next** until you reach the final window of the Create Web Module Wizard. Click **Finish**.

After you close both wizards, go to **File -> Save As** in the Application Assembly Tool window, and type the name of your WAR file in the File name field. Be sure that the file extension of your file is .war. Save your WAR file in the WebSphere\Appserver\InstallableApps directory (Figure 18-7).

Once you save your file, a window appears that tells you that it was saved successfully. Click **OK**, and close out of the Application Assembly Tool.



Look in: installableApps

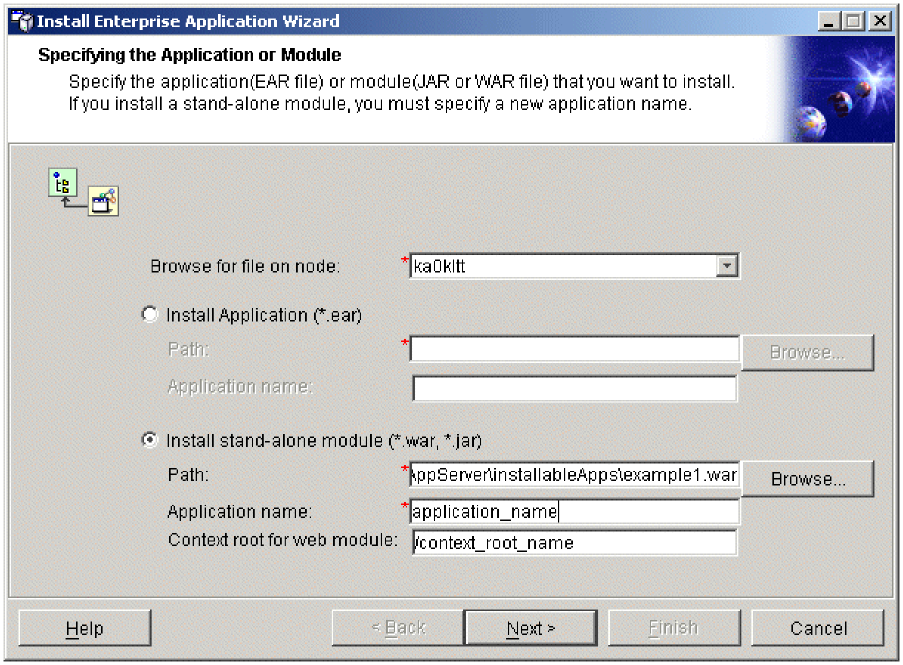
File name: example1.war

Files of type: J2EE archive (*.war,*.ear,*.jar)

Figure 18-7 Save WAR file

15. Open the Administrative Console by selecting **Start -> Programs -> IBM WebSphere -> Application Server V4.0 AE -> Administrator's Console**. Be sure that the administration server is running, or you will get an error message. To start the administration server, go to **Programs -> IBM WebSphere -> Application Server V4.0AE -> Start Admin Server**.

16. Once the Administrative Console is open, go to the Console drop-down menu and select **Wizards -> Install Enterprise Application**. In the Specifying the Application or Module window (Figure 18-8), select **Install stand-alone module (*war, *jar)**. By default, the name of your local host appears in the Browse for file on node field.



Install Enterprise Application Wizard

Specifying the Application or Module

Specify the application(EAR file) or module(JAR or WAR file) that you want to install.
If you install a stand-alone module, you must specify a new application name.

Browse for file on node: * ka0kltt

○ Install Application (*.ear)

Path: *

Application name:

● Install stand-alone module (*.war, *.jar)

Path: * ppServer\installableApps\example1.war

Application name: * application_name

Context root for web module: /context_root_name

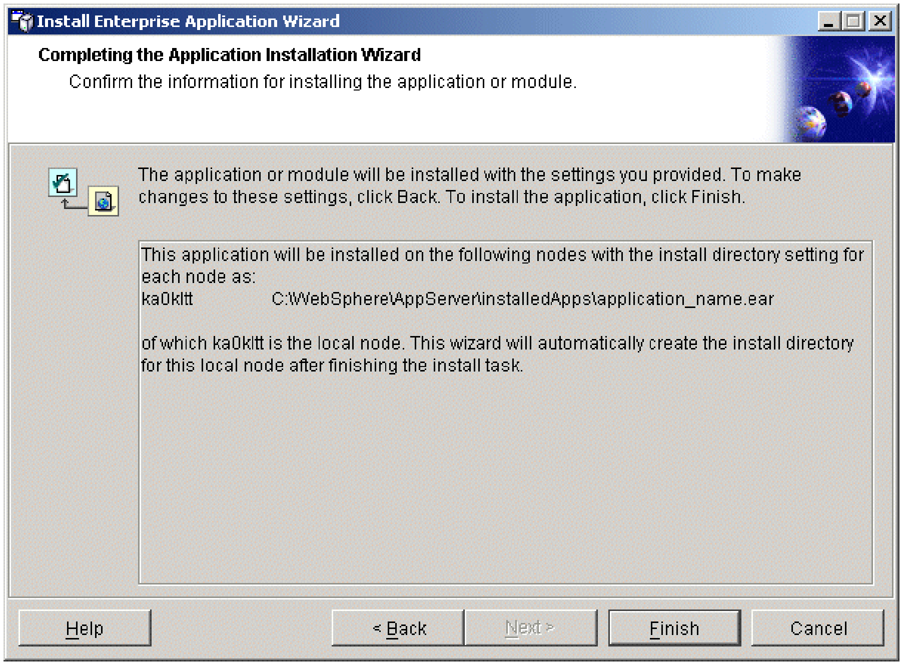
Figure 18-8 Specifying the Application or Module

Type the Path, Application name, and Context root for Web module:

- For Path, browse to the WebSphere\Appserver\InstallableApps directory and select the WAR file that you saved in Step 14. on page 647.
- For Application name, type the name of the application. This will be the name of the EAR file that WebSphere creates later.
- For the Context root for Web module, type the name of the context root. The first character must be a backwards slash (/). The context root is the part of the session URL that comes immediately after the host name, for example, `http://host_name/context_root_name/FileName.jsp`.

Click **Next**.

17. Continue clicking through several windows until you reach the last window of the Install Enterprise Application Wizard (Figure 18-9). At this point, you are installing the Web module, which will be placed into an EAR file and expanded in the installedApps directory. This is the final stage before the application is actually deployed. Click **Finish**.



Completing the Application Installation Wizard

Confirm the information for installing the application or module.

The application or module will be installed with the settings you provided. To make changes to these settings, click Back. To install the application, click Finish.

This application will be installed on the following nodes with the install directory setting for each node as:
ka0kltt C:\WebSphere\AppServer\installedApps\application_name.ear

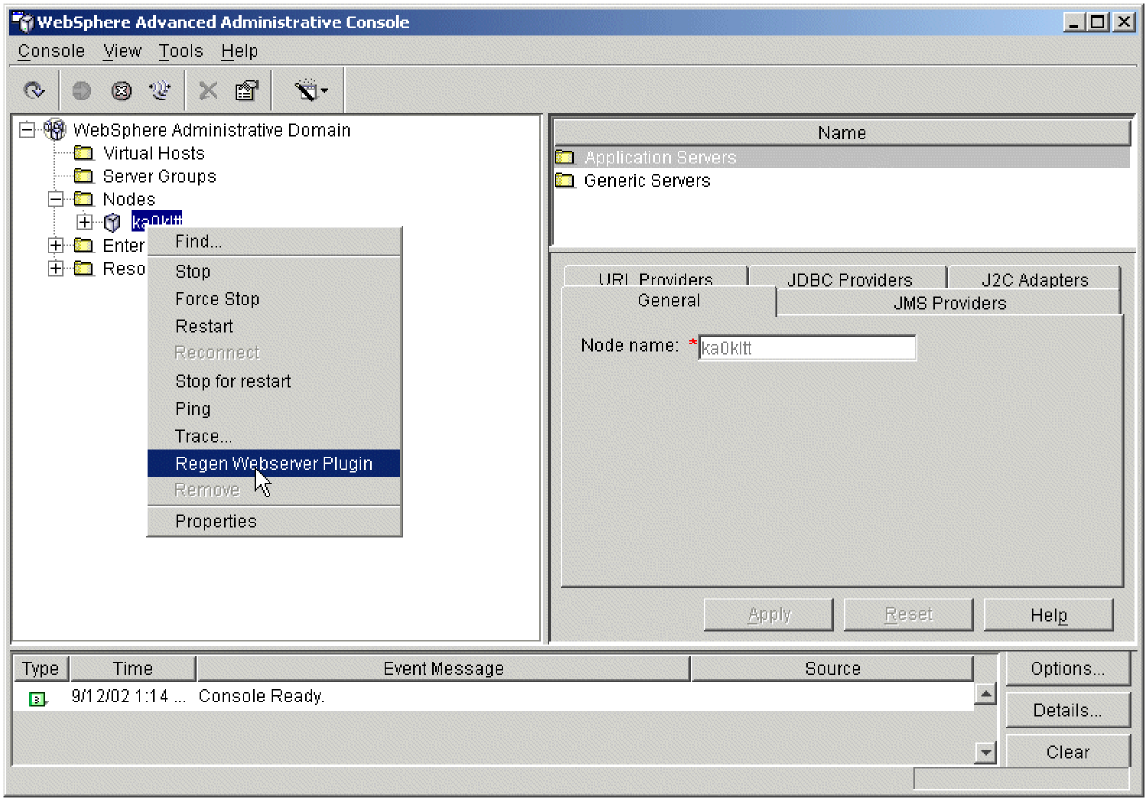
of which ka0kltt is the local node. This wizard will automatically create the install directory for this local node after finishing the install task.

Figure 18-9 Completing the Application Installation Wizard

If completed successfully, an information dialog appears. Click **OK** and close the Administrative Console.

18. Since you have changed certain WebSphere configuration properties, you must regenerate the Web server plug-in configuration. Open the Administrative Console by selecting **Start -> Programs -> IBM WebSphere -> Application Server V4.0 AE -> Administrator's Console**.

    In the left navigation bar, select the plus sign (**+**) to expand Nodes. Right-click your local host and select **Regen Webserver Plug-in** (Figure 18-10). You will not see any visual indication that the plug-in is regenerating, but you will know when it completes the regeneration process by viewing the **Event Message Log** in the bottom frame of the Administrative Console. Regenerating the plug-in usually takes a few minutes.



Node name: * ka0kltt

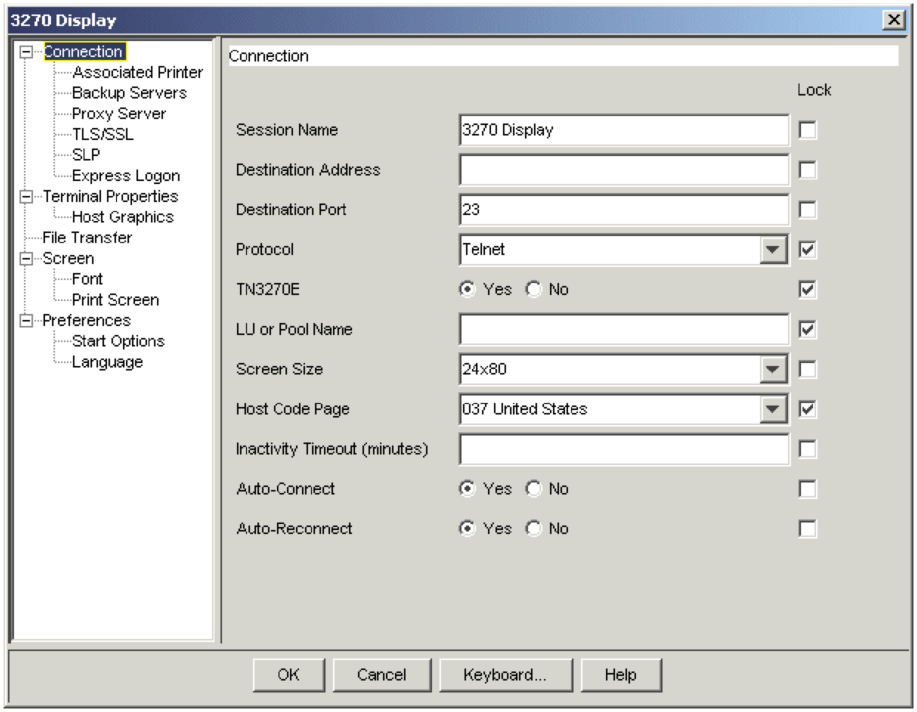
Type	Time	Event Message	Source
	9/12/02 1:14 ...	Console Ready.	

Figure 18-10 Regen Webserver Plug-in

Important: If your Web server is on a separate machine, then you will have to move the plugin-cfg.xml file to the Web server machine after the plug-in regeneration. This file is located in the WAS_ROOT/AppServer/config directory.

19. Stop and restart WebSphere and your Web server. To stop WebSphere, go to **Start -> Settings -> Control Panel -> Administrative Tools -> Services -> IBM WS AdminServer 4.0**. Right-click **IBM WS AdminServer 4.0** and select **Stop**. Once the administration server stops, right-click **IBM WS AdminServer 4.0** and select **Start**. It usually takes a few minutes to complete this process.

20. Finally, point your browser to `http://your_host/context_root_name/FileName.jsp` and retrieve the Host On-Demand session. In the URL, your_host is the name of your local host, context_root_name is the name of the context root, and FileName.jsp is the name of your JSP file. Once the session icon appears, right-click the icon and select **Properties**. In the **Connection** tab (Figure 18-11), check to make sure that the LU name that you specified in luname.table for your IP address is in the LU or Pool Name field on the window.



Connection

		Lock
Session Name	3270 Display	□
Destination Address		□
Destination Port	23	□
Protocol	Telnet	☑
TN3270E	● Yes ○ No	☑
LU or Pool Name		☑
Screen Size	24x80	□
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)		□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 18-11 Connection tab of Deployment Wizard session properties

18.4.2 Troubleshooting: Scenario 1

If your HTML override is not successful, take the following steps to help determine the cause:

1. Use a static value in your HTML file to see if your HTML overrides mechanism is working. For example, instead of coding the HTML file so that the IP address of the user and the corresponding LU name are looked up from the luname.table file (Step 2), replace the table lookup with a static LU name value, as in the following example:

   ```
   document.write('<PARAM NAME="Luname" VALUE="3270
       Display=Static_LU_name">');
   ```

   Refer to 4 on page 654 to see where these lines are located in the JSP file.

   Once you complete the steps to override the HTML parameter, open the session properties, and make sure that the static LU name is in the LU, or Pool Name field of the Connection tab.

2. Add the debug parameter DebugCode to your HTML file generated by the Deployment Wizard, and set it to a value of 65535:

   ```
   document.write('<PARAM NAME="DebugCode" VALUE="65535">');
   ```

   This parameter sends useful debugging information to the Java Console, such as whether or not your Codebase, ConfigBase, and TargetedSessionList parameters and session properties were read correctly.

   Refer to 6 on page 654 to see where this line is located in the JSP file.

3. Check your access log file for messages that contain the code 404. This is the standard code for “Page Not Found.” This access log file is generated by your Web server and is located in your Web server directory.

18.4.3 Completed HTML file after edits

The following code is the original HTML code generated from the Deployment Wizard plus the additions the administrator made to the modify session properties dynamically. The lines added to the original file are displayed in bold. The callout boxes in the left margin show you the corresponding step from the previous section.

Example 18-1 Deployment Wizard plus additions

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">

<%
java.util.Properties lunames = new java.util.Properties();
lunames.load(new java.io.FileInputStream("c:\\luname.table"));
%>
```

1

```
<!-- HOD WIZARD HTML -->
<HTML>
<HEAD>
<META content="text/html; charset=UTF-8">
<!-- TITLE Begin -->
<TITLE>Example1</TITLE>
<!-- TITLE End -->
<!-- SUMMARY Begin -->
<!--
Configuration Model
   What configuration model would you like to use?
   -HTML-based model
Sessions created
   -3270 Display
   -5250 Display
Additional Options
   -Allow users to save session changes? = True
   -Cached = True
   -Java Type = java1
Disable Functions
Preload Options
   -5250 Sessions = True
   -Change Session Properties = True
   -FTP Sessions = True
   -3270 Sessions = True
Server Connection Options
Cache Options
   Basic Options
   -Debug = False
   -Height (in pixels) = 250
   -Width  (in pixels) = 550
   Cache Client Upgrade Option
   -Percent of users who can upgrade by default = 100
   -Prompt user (user decides foreground or background)
Advanced Options
   Display
   -Standard Host On-Demand Client
   -Applet size = Autosize to browser
   -Maximum sessions = 26
   Other
   -Locale = Use the system Locale
   -Debug = False
   -HTML Template = Default
   Additional Parameters
   -None
-->
<!-- SUMMARY End -->
</HEAD>
```

```
    <BODY BACKGROUND="hodbkgnd.gif">
    <CENTER>
    <IMG src="hodlogo.gif" ALT="hodlogo.gif">
    <P>

    <SCRIPT LANGUAGE="JavaScript">
    function writeAppletParameters()
    {
       document.write("");
    }
    </SCRIPT>

    <SCRIPT LANGUAGE="JAVASCRIPT" SRC="CachedJ1.js"></SCRIPT>
    <SCRIPT LANGUAGE="JAVASCRIPT">
    var hod_Height='80%';
    var hod_Width='80%';
    document.write('<APPLET ARCHIVE="CachedAppletSupporter.jar" MAYSCRIPT
    NAME="HODApplet"
    CODE="com.ibm.eNetwork.HOD.cached.appletloader.CachedAppletLoader"
    WIDTH="'+hod_Width+'" HEIGHT="'+hod_Height+'">');
    document.write('<PARAM NAME="Cabinets"
    VALUE="CachedAppletSupporter.cab">');
    document.write('<PARAM NAME="CachedClient"             VALUE="true">');
    document.write('<PARAM NAME="ParameterFile"
    VALUE="HODData\\Example1\\params.txt">');
    document.write('<PARAM NAME="JavaScriptAPI" VALUE="false">');

2   document.write('<PARAM NAME="EnableHTMLOverrides" VALUE="true">');

3   document.write('<PARAM NAME="TargetedSessionList"
        VALUE="3270 Display,5250 Display">');

4   document.write('<PARAM NAME="Luname" VALUE="3270
       Display=<%=lunames.get(request.getRemoteAddr())%>">');

5   document.write(‘<PARAM NAME=”ConfigBase”
       VALUE=”http://host_name/hod/”>’);

6   document.write(‘<PARAM NAME=”DebugCode”
       VALUE=”65535”>’);

    writeAppletParameters();
    document.write("</APPLET>");
    </SCRIPT>

    <P>
    <SCRIPT LANGUAGE="JavaScript">
    var hod_AppName='';
    var hod_Preloadlist='HABASE;HODBASE;HODIMG;HACP;HAFNTIB;
        HAFNTAP;HA3270;HODCFG;HAFTP;HA5250';
    var hod_Debugcomponents='false';
    var hod_Debugcachedclient='false';
    var hod_Upgradepromptresponse='Prompt';
    var hod_Upgradepercent='100';
    var hod_Framewidth='550';
    var hod_Frameheight='250';

    function isBookmark(mySearch) {
      if (mySearch.length < 2) {
        return false;
      } else {
        return (mySearch.toLowerCase().indexOf('launch=') != -1);
      }
    }

    if (hod_AppName == '') {
      if (isBookmark(window.location.search.substring(1)))
        hod_AppName = 'com.ibm.eNetwork.HOD.SessionLauncher';
      else
        hod_AppName = 'com.ibm.eNetwork.HOD.HostOnDemand';
    }
    function getHODFrame() {
      return self;
    }
    document.write('<APPLET ARCHIVE="CachedAppletSupporter.jar" MAYSCRIPT
    NAME="CachedAppletSupporter"
    CODE="com.ibm.eNetwork.HOD.cached.appletsupport.CachedAppletSupportApplet"
    WIDTH="2" HEIGHT="2">');
    document.write('<PARAM NAME="Cabinets"
    VALUE="CachedAppletSupporter.cab">');
    document.write('<PARAM NAME="DebugComponents"
    VALUE="'+hod_Debugcomponents+'">');
    document.write('<PARAM NAME="PreloadComponentList"
    VALUE="'+hod_Preloadlist+'">');
    document.write('<PARAM NAME="DebugCachedClient"
    VALUE="'+hod_Debugcachedclient+'">');
    document.write('<PARAM NAME="CachedClientSupportedApplet"
    VALUE="'+hod_AppName+'">');
    document.write('<PARAM NAME="InstallerFrameWidth"
    VALUE="'+hod_Framewidth+'">');
    document.write('<PARAM NAME="InstallerFrameHeight"
    VALUE="'+hod_Frameheight+'>"');
    document.write('<PARAM NAME="UpgradePromptResponse"
    VALUE="'+hod_Upgradepromptresponse+'">');
    document.write('<PARAM NAME="UpgradePercent"
    VALUE="'+hod_Upgradepercent+'">');
    document.write('</APPLET>");
    </SCRIPT>
```

```
</CENTER>
</BODY>
</HTML>
```

18.5 Scenario 2: Specifying the host name using an HTML form

A company decides to display a simple form that prompts its Host On-Demand client users to enter the host name. The administrator uses HTML overrides so that the host name entered by the user overrides the host name that was configured in the 3270 host session. In this case, the HTML form posts to a JSP program, which stores and uses the form data to override the host name.

In the following section, we provide the steps that this administrator takes to modify session properties dynamically, including editing the Deployment Wizard HTML file, creating a simple HTML file that users can enter their host names, and deploying the JSP. Because the administrator has already followed the steps in 18.4, “Scenario 1: Overriding the LU name based on client IP address” on page 637, there is no need to recreate a Web module using WebSphere Application Server. This means one can simply save the JSP file to the same directory where the JSP file was deployed in Scenario 1.

Once we show you the steps this administrator takes to modify session properties dynamically, we show you an example of the completed JSP code and offer troubleshooting advice.

Note: The following instructions are specific for this company’s environment, which includes a Windows 2000 operating system and IBM WebSphere Application Server Advanced Edition Version 4.0. Other environments may require additional steps.

18.5.1 Steps to modify the session properties

Follow these steps in order to display a simple form that allows users to enter in their host name and override the host name specified in the session properties:

1. Use the Deployment Wizard to set up your initial HTML file. On the Additional Options window, click **Advanced Options** and go to the **Other** tab. Type the relative path `/hod/` in the Codebase field (Figure 18-1). Save the HTML file to the default Host On-Demand publish directory `HostOnDemand/HOD`. Your HTML file is now in the same directory with Host On-Demand’s archive files.

Important: Codebase refers to the installed Host On-Demand publish directory, not the directory where you publish your Deployment Wizard files. Although you can enter a fully qualified URL in the Codebase field, we strongly recommend that you enter the relative path /hod/ for the default publish directory when modifying session properties dynamically. If you enter a fully qualified URL, any users who specify the host name in a different manner than you specified as the Codebase will not be able to access the files, even if the DNS entries resolve to the same IP address.

For more information about Codebase and which files are created by the Deployment Wizard, refer to Chapter 14., “Deployment Wizard” on page 517.

Take note of the following points:

- The Deployment Wizard generates some of the HTML using JavaScript, and the HTML parameters are specified within a JavaScript array or by means of JavaScript document.write statements.
- The format of the HTML code generated by the Deployment Wizard depends on whether you select Java 1, Java 2, or Autodetect for the Client Java Type and whether or not you select to cache the Host On-Demand applet on your users' machines. Both of these options are located on the Additional Options window of the Deployment Wizard. (This scenario uses a non-cached Autodetect HTML file.)

2. Use the following code to create a simple HTML form called HODForm.html that allows users to input their host names. The form posts to a JSP program called example2.jsp. Save this file to the default Host On-Demand publish directory HostOnDemand/HOD.

Example 18-2 HODForm.html

```
<form method="POST"  action="context_root/example2.jsp">
Hostname <input name="form.hostname"><br>
<input type="submit">
</form>
```

Figure 18-12 shows what the HTML file looks like in a browser.

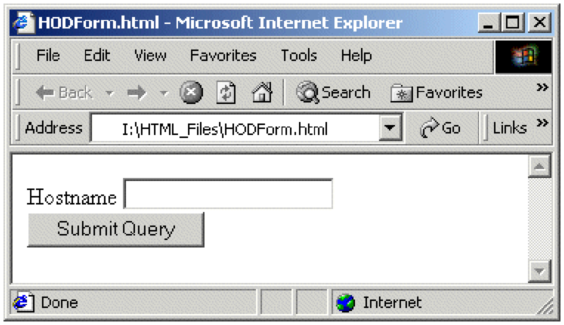

HODForm.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
I:\HTML_Files\HODForm.html
Go
Links
Hostname
Submit Query
Done
Internet

Figure 18-12 Browser view of HODForm.htm

3. The following steps require you to edit your Deployment Wizard HTML code:

   a. Get a session and store the host name that the user enters into the form by including the following code in your Deployment Wizard file:

   ```
   HttpSession session = request.getSession(true);
   String hostname = request.getParameter("form.hostname");

   if (hostname!=null) {
       session.putValue("session.hostname", hostname);
   }
   ```

   Refer to 1 on page 662 to see where this code is located in the JSP file.

   When using forms, the form data needs to be retained across requests to the program. This is because Host On-Demand HTML files reload themselves for Java detection and for bookmarking support. If Java 1 is selected and bookmarking support is disabled if using the configuration server-based model, the page will not need to reload and there is no need to retain the form data.

   b. In the following line, change `z_example2.html` to `z_example2.jsp`, where `example2.html` is the name of your Deployment Wizard file:

   ```
   var hod_FinalFile = ‘z_example2.jsp’;
   ```

   Refer to 2 on page 663 to see where this line is located in the JSP code.

   c. If you want a JavaScript alert window to appear when you first access the JSP file that tells you if your program generated the proper syntax, change false to true in the following line:

   ```
   var hod_DebugOn = true;
   ```

   Refer to 3 on page 663 to see where this line is located in the JSP code.

d. Enable HTML overrides by including the EnableHTMLOverrides parameter in your HTML file and setting it to a value of true, as in the following example:

```
hod_AppletParams[4] = '<PARAM NAME="EnableHTMLOverrides" VALUE="true">';
```

Refer to 4 on page 663 to see where this line is located in the JSP code.

e. List the sessions to be overridden by including the TargetedSessionList parameter and setting the value as the exact names of the sessions that you are modifying dynamically. Since you may have multiple sessions associated with your HTML file, you need to specify which sessions you are modifying.

In the following example, the administrator set the value as the list of session names (3270 Display and 5250 Display) and separated them with commas:

```
hod_AppletParams[5] = '<PARAM NAME="TargetedSessionList"
 VALUE="3270 Display,5250 Display">';
```

Refer to 5 on page 663 to see where these lines are located in the JSP code.

f. Change the host or destination address session parameter for the session named 3270 Display. In the following example, the host is set to the value saved in the JSP session from the HTML form:

```
hod_AppletParams[6] = '<PARAM NAME="Host" VALUE="3270
  Display=<%=session.getValue("session.hostname")%>">';
```

Refer to 6 on page 663 to see where these lines are located in the JSP code.

Tip: When you are initially testing your changes, you may want to use a constant value to verify that the syntax is correct before you insert a calculated value.

g. Add a ConfigBase parameter to the JSP file:

```
hod_AppletParams[7] = '<PARAM NAME="ConfigBase"
   Value="http://host_name/hod/">');
```

Important: As with defining `/hod/` as the Codebase in Step 1, the ConfigBase parameter is necessary because you will eventually deploy your JSP file to a location that is different than the default publish directory, and the Host On-Demand applet needs to know how to find the session configuration files located in the `HostOnDemand/HOD/HODData` directory. These files are created at the same time you save your Deployment Wizard HTML file to the publish directory.

Unlike Codebase, the ConfigBase parameter requires a fully qualified URL. ConfigBase is a term that is specific to Host On-Demand.

For more information, refer to 14.5, “Files created by the Deployment Wizard” on page 548.

Refer to **7** on page 663 to see where this line is located in the JSP code.

h. Find the z_example2.html file, where `example2.html` is the name of your Deployment Wizard HTML file that you created in Step 1, and change the file extension to .jsp. This file is located in the HostOnDemand/HOD directory. Open it and copy it to the same directory that you deployed the other JSP files that you created to override session properties. The reason you must manually copy this file is because the ConfigBase parameter does not affect this file.

i. Compare your new HTML code to make sure that it is identical to the code in the file provided in 18.5.2, “Troubleshooting: Scenario 2” on page 661. If not, make the necessary changes. If so, change the file extension from HTML to JSP and save it to the same directory where you keep the other JSP files that you have created to override session properties.

Important: This scenario assumes that you have already created a Web module using WebSphere Application Server. If you have not already created a Web module, repeat steps 9-19 in 18.4.1, “Steps to modify the session properties” on page 638.

4. Finally, point your browser to the form at `http://your_host/context_root/HODForm.html`, where your_host is the name of your local host and context_root is the name of the context root. Once the form appears and you enter and submit your host name, the browser redirects to the JSP file, and the session icon appears. Right-click the session icon and select **Properties**. In the **Connection** tab (Figure 18-11), check to make sure that the host name you specified in the form is located in the Destination Address field.

18.5.2 Troubleshooting: Scenario 2

If your HTML override is not successful, take the following steps to help determine the cause:

1. Use a static value in your HTML file to see if your HTML overrides mechanism is working. For example, instead of coding the HTML file so that the host name comes from the `HODForm.html` (Step 2), replace the form lookup with a static host name value, as in the following example:

   ```
   hod_AppletParams[4] = '<PARAM NAME="Host" VALUE="3270
      Display=Static_host_name">');
   ```

   Refer to 4 on page 663 to see where these lines are located in the HTML file.

   Once you complete the steps to override the HTML parameter, open the session properties and make sure that the static host name is in the Destination Address field of the Connection tab.

2. If you want a JavaScript alert window to appear when you first access the JSP file that tells you if your program generated the proper syntax, change false to true in the following line:

   ```
      var hod_DebugOn = true;
   ```

   Refer to 3 on page 663 to see where this line is located in the HTML code.

3. Add the debug parameter DebugCode to your HTML file generated by the Deployment Wizard and set it to a value of 65535:

   ```
   document.write('<PARAM NAME="DebugCode" VALUE="65535">');
   ```

   This parameter sends useful debugging information to the Java Console, such as whether or not your Codebase, Configbase, and TargetedSessionList parameters and session properties were read correctly.

   Refer to 8 on page 663 to see where this line is located in the HTML file.

4. Check your access log file for messages that contain the code '404'. This is the standard code for “Page Not Found.” This access log file is generated by your Web server and is located in your Web server directory.

18.5.3 Completed HTML file after edits

The following code is the original HTML code generated from the Deployment Wizard plus the additions the administrator made to modify session properties dynamically. The lines added to the original file are displayed in bold. The callout boxes in the left margin show you the corresponding step from the previous section.

Example 18-3   Deployment Wizard output with additions

```
<%
HttpSession session = request.getSession(true);          1
String hostname = request.getParameter("form.hostname");

if (hostname!=null) {
    session.putValue("session.hostname", hostname);
}
%>
<HTML>
<!-- HOD WIZARD HTML -->
<HEAD>
<META content="text/html; charset=UTF-8">
<TITLE>example2</TITLE>
<!-- SUMMARY Begin -->
<!--
Configuration Model
   What configuration model would you like to use?
   -HTML-based model
Sessions created
   -3270 Display
   -5250 Display
Additional Options
   -Allow users to save session changes? = True
   -Cached = False
   -Java Type = detect
Disable Functions
Preload Options
   -5250 Sessions = True
   -Change Session Properties = True
   -3270 Sessions = True
Server Connection Options
Cache Options
Advanced Options
   Display
   -Standard Host On-Demand Client
   -Applet size = Autosize to browser
   -Maximum sessions = 26
   Other
   -Locale = Use the system Locale
   -Debug = False
   -HTML Template = Default
   Additional Parameters
   -None
-->
<!-- SUMMARY End -->
</HEAD>
<SCRIPT LANGUAGE="JAVASCRIPT" SRC="CommonJars.js"></SCRIPT>
```

```
     <SCRIPT LANGUAGE="JAVASCRIPT" SRC="HODJavaDetect.js"></SCRIPT>
     <SCRIPT LANGUAGE="JAVASCRIPT" SRC="CommonParms.js"></SCRIPT>
     <SCRIPT LANGUAGE="JAVASCRIPT">

     //---- Start JavaScript variable declarations ----//
     var hod_Locale = '';
     var hod_AppName ='';
     var hod_AppHgt = '80%';
     var hod_AppWid = '80%';
     var hod_CodeBase = '/hod/';
2    var hod_FinalFile = 'z_example2.jsp';
     var hod_JavaType = 'detect';
     var hod_Obplet = '';
     var hod_jars =
     'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hodsignn.jar,
          ha3270n.jar,hodcfgn.jar,ha5250n.jar';

     var hod_URL = new String(window.location);
3    var hod_DebugOn = true;
     var hod_SearchArg = window.location.search.substring(1);

     var hod_AppletParams = new Array;
     hod_AppletParams[0] = '<PARAM NAME="ParameterFile"

     hod_AppletParams[0] = '<PARAM NAME="ParameterFile"
          VALUE="HODData\\example2\\params.txt">';
     hod_AppletParams[1] = '<PARAM NAME="ShowDocument"  VALUE="_parent">';
     hod_AppletParams[2] = '<PARAM NAME="JavaScriptAPI" VALUE="false">';
     hod_AppletParams[3] = '<PARAM NAME="PreloadComponentList"
     VALUE="HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HA3270;HODCFG;HA5250">';

4    hod_AppletParams[4] = '<PARAM NAME="EnableHTMLOverrides" VALUE="true">';

5    hod_AppletParams[5] = '<PARAM NAME="TargetedSessionList"
         VALUE="3270 Display,5250 Display">';

6    hod_AppletParams[6] = '<PARAM NAME="Host" VALUE="3270
         Display=<%=session.getValue("session.hostname")%>">';

7    hod_AppletParams[7] = '<PARAM NAME="ConfigBase"
        Value="http://host_name/hod/">');

8    hod_AppletParams[8] = '<PARAM NAME="DebugCode" VALUE="65535">';

     var lang = detectLanguage(hod_Locale);

     function getHODMsg(msgNum) {
       return HODFrame.hodMsgs[msgNum];
     }
```

```
//---- End JavaScript variable declarations ----//

function getHODFrame() {
  return HODFrame;
}

document.writeln('<FRAMESET cols="*,10" border=0 FRAMEBORDER="0">');
document.writeln('<FRAME    src="hoddetect_' + lang + '.html"
name="HODFrame">');
document.writeln('</FRAMESET>');
</SCRIPT>
</HEAD>
</HTML>
```

19

Host On-Demand portlets

In this chapter we cover the support in Host On-Demand for IBM WebSphere Portal. This support allows Host On-Demand to run as a portlet within the Portal Server component of WebSphere Portal.

19.1 Introduction to WebSphere Portal

IBM WebSphere Portal provides a single point of access to applications, application content, processes, and people in your network.

19.1.1 What is a portal?

Portals provide a secure, single point of interaction, with diverse information, business processes, and people, which is personalized to a user's needs and responsibilities. The single point of interaction is the dominant characteristic identified by portal users:

- Personalization for end user's is a critical feature - A portal must deliver a personal or community desktop to users by establishing unique looks, content, and application interfaces, and operatively rendering them based on the user's role in their community, or by actively tracking the user's individual usage, interests, and behaviors.
- Organization of the user's desktop to eliminate the information glut - Users want consolidated access to their important contacts, applications, and content. The concept of stovepipe applications are a thing of the past. Organizations want easier control to design their desktop in a layout that suits them.
- Resource division determines who sees what - Portals must have a membership services layer for user authentication, single-logon and credential mapping. Users demand the highest level of security, but the least amount of annoyance.
- Tracking of activity provides users with a payback for using the portal - The more users use the portal, the more it becomes tailored to specific interests and affinities the user may develop. While this may sound threatening at first, users will have the ultimate control over what gets tracked.
- Access and display of aggregated multiple heterogeneous data stores - This includes relational databases, multidimensional databases, document management systems, e-mail systems, Web servers, news feeds, and various file systems/servers (for example, audio, video, image, and so on). It is extremely helpful for users to see their e-mail, next to news feeds, beside a list of online users who can help understand information while maintaining a single context.
- Location of important people and things - A portal is based on the basic desire of users to easily find information and people by searching or navigation. There must be a means of passively or actively discovering the experts, communities, and content in a relevant context. If developers succeed in incorporating all these capabilities into a single application they have built a

basic portal design that can be targeted at all types of audiences, and applied against a broad range of content and tool types.

19.1.2 Overview

IBM WebSphere Portal allows you to establish customized portals for your employees, Business Partners, and customers. As illustrated in Figure 19-1, the framework architecture implemented in this product provides a unified access point to internal and external Web applications as well as portal access to other legacy applications. In this way, users sign on to the portal and receive personalized Web pages.

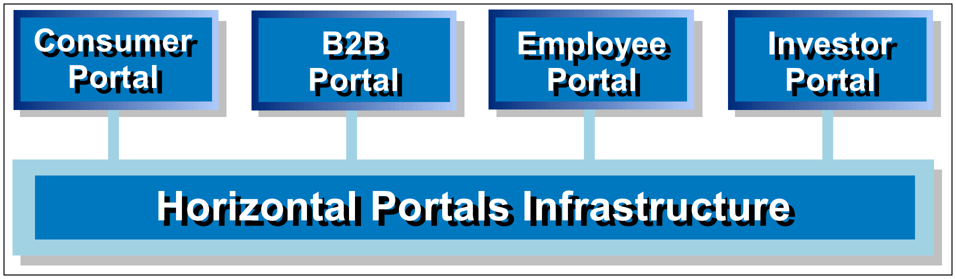


Figure 19-1 Portals horizontal and vertical framework

The personalized single point of access to all necessary resources reduces information overload, accelerates productivity, and increases Web site usage. In addition, portals do much more; for example, they provide additional valuable functions such as security, search, collaboration and workflow.

A portal delivers integrated content and applications, plus a unified, collaborative workplace. Portals are the next-generation desktop, delivering e-business applications over the Web to all kinds of client devices.

IBM WebSphere Portal has been designed in response to the following set of fundamental business objectives:

- A single point of access to all resources associated with the portal domain
- Personalized interaction with the portal services
- Federated access to hundreds of data types and repositories, aggregated and categorized
- Collaboration technologies that bring people together
- Integration with applications and workflow systems

IBM as well as some industry analysts have focused on the concept of horizontal and vertical portals. Horizontal portals are the primary infrastructure upon which a portal is built. Vertical portals are built upon the horizontal layer and represent a specific portal instance, usually defined by a major topic or domain.

As illustrated in Figure 19-2, the horizontal portal infrastructure consists of several modular subsystems including the following:

- Presentation layer - a Web user interface plus pervasive device support
- Personalization - the ability to serve dynamic response to the user based on personal profiles
- Collaboration - tools that allow e-mail, team rooms, shared places, etc. to be exchanged
- Portlets - a framework for easily attaching software modules (portlets) and services, for example Host On-Demand portlets
- Applications and workflow - integration of legacy and new applications
- Search and navigation - categorizing repositories of content and searching them for relevant information
- Publish and subscribe - the ability to author new content and publish it to subscribers
- Administration and security - basic Web site services such as page designers, performance monitors, cluster services, and metadata management
- Integration - metadata sharing, XML, connectors, standards, EAI

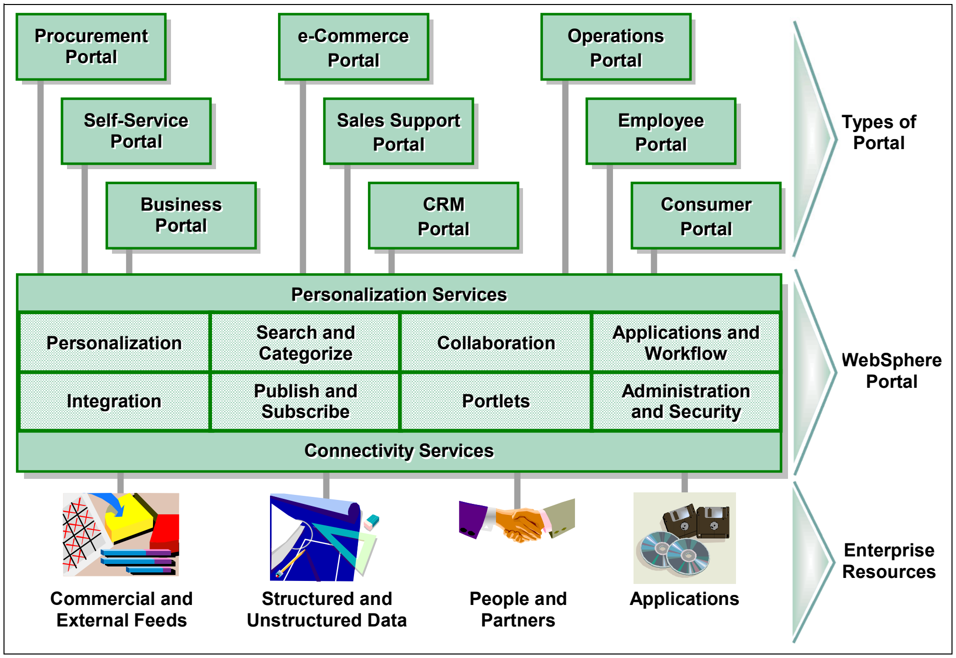


Figure 19-2 WebSphere Portal architecture

WebSphere Portal provides additional services such as single sign-on, security, Web content publishing, search and, personalization, collaboration services, enterprise application integration, support for mobile devices, and site analysis.

Note: WebSphere Portal provides an extensible framework for interacting with enterprise applications, content, people, and processes. Self-service features allow end users to personalize and organize their own view of the portal, to manage their own profiles, and to publish and share documents with their colleagues.

19.1.3 The WebSphere Portal infrastructure

IBM WebSphere Portal provides a framework that breaks the different portal components into portlets to accommodate the aggregation and display of diverse content. Each portlet is responsible for accessing content from its source (for example, a Web site, database, or e-mail server) and transforming the content so that it can be rendered to the client.

From a user's perspective, a portlet is a small window in the portal that provides a specific service or information. From an application development perspective, portlets are pluggable modules that are designed to run inside a portlet container of a portal server. The portlet container provides a runtime environment in which portlets are installed and used.

Portlets rely on the portal infrastructure to access user profile information, participate in window and action events, communicate with other portlets, access remote content, look up credentials, and store persistent data. The portlet API provides standard interfaces for these functions.

The portlet container is not a stand-alone container like the servlet container. Instead, it is implemented as a thin layer on top of the servlet container and reuses the functionality provided by the servlet container.

19.1.4 What is a portlet

Portlets are reusable components that provide access to enterprise applications, Web-based content, and other resources. For example, Web pages, Web services, syndicated content feeds, and legacy host applications can be accessed through portlets.

Any particular portlet is developed, deployed, managed, and displayed independent of other portlets. Administrators and end users create personalized portal pages by choosing and arranging portlets, resulting in Web pages.

Many portlets are available from IBM. The Host On-Demand portlet is one of them.

19.1.5 Information on IBM Portal Servers

IBM provides a tremendous amount of documentation on configuring IBM Portal Servers.

Search the IBM redbook site for Portal:

`http://redbooks.ibm.com`

Search the IBM Web site for Portal Products:

`http://www.ibm.com/software/webservers/portal/`

19.2 HOD portlet with WebSphere Portal

The following figure illustrates how Host On-Demand works with Portal Server.

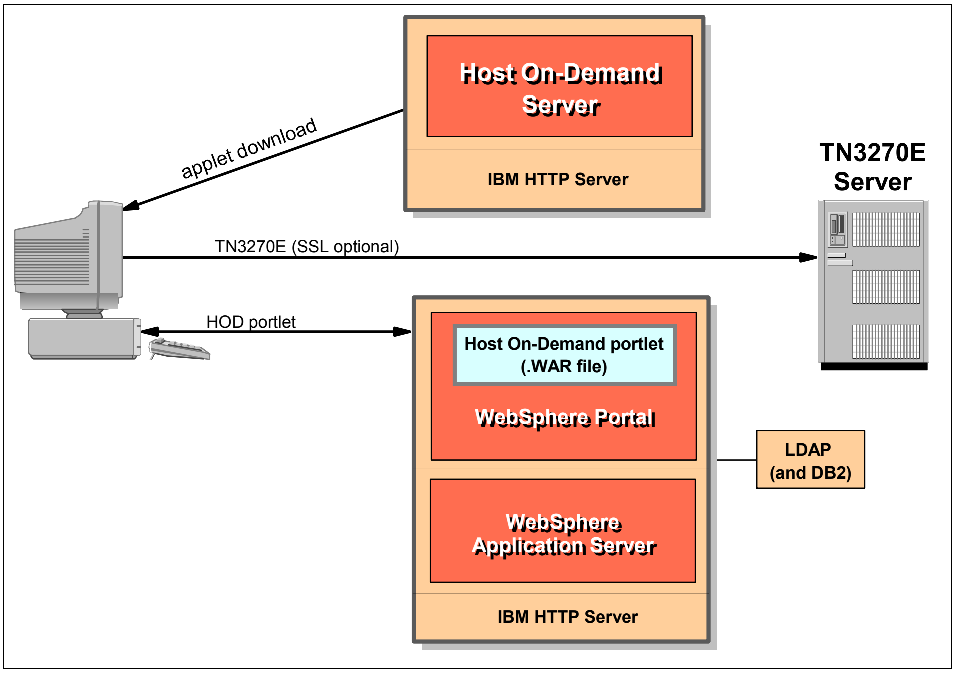


Figure 19-3 Host On-Demand with WebSphere Portal

- A user logs into the portal through a browser. If the HOD portlet is on a public page, user sign-on to the Portal Server may not be required. Otherwise, the user is authenticated by a user ID and password.
- The set of portlets customized for the user is downloaded to the user's machine and displayed in the browser.
- If a Host On-Demand portlet is configured for the user, Host On-Demand starts. The client receives the applet from the Host On-Demand server. The Host On-Demand server address is configured by the Portal Server administrator during the deployment process for this HOD portlet. The user may also have to provide a user ID and password to login to HOD.
- The Host On-Demand applet makes a connection to a destination Telnet server. The configuration values required to access all the required Telnet severs, such as IP address, port, and SSL configuration, are defined in the portlet.

19.3 Scenarios for Host On-Demand portlets

Business-to-business (B2B)

B2B portals are usually designed to support and conduct business transactions over the Internet, especially between business partners who are connected through an extranet. Security enforcement and XML support are critical success factors.

In a well-controlled B2B environment, you can use the Host On-Demand portlet to implement direct access to the host applications on your B2B portal. This allows your business partners to use your host business applications directly without any change. Firewalls might be an issue for some enterprises because to use Host On-Demand across enterprise boundaries, you usually need to open a special port on the firewalls that allow Telnet-based communication between HOD applets on the browser and the host.

Business-to-employee (B2E)

A sophisticated B2E portal must address a number of requirements:

- Support collaboration and communities
- Provide capability of knowledge management to share valuable intellectual assets between employees
- Allow users to do business intelligence
- Enable legacy or host integration

An intranet is typically a secure environment with high-speed networking. Most of the employees are power users; some of them may know the existing host applications well. In this case, Host On-Demand portlets can be a foundation for providing the capability of accessing host applications through a portal without any change of host applications. You can deploy the integration solution quickly. Users who are acquainted with host applications can start using the portal solution without any significant education.

To leverage the capability of single sign-on provided by the Portal Server, you should consider using Windows domain logon for client authentication if possible, and the Certificate Express Logon for host application authentication, so that from the user's point of view, access to host applications through the portal is also well-integrated in the portal single sign-on security environment.

Business-to-consumer (B2C)

A portal provides one easy to use, attractive interface to your corporate business applications from any location in the world. The Host On-Demand portlet can provide a favorable first impression of your company to your customers.

Using the single sign-on of the Portal Server infrastructure to enable the security check for the host applications is highly recommended.

19.4 Host On-Demand portlet generation

Host On-Demand portlets support IBM Websphere Portal for Multiplatforms V2.1, V4.1, and V4.2.

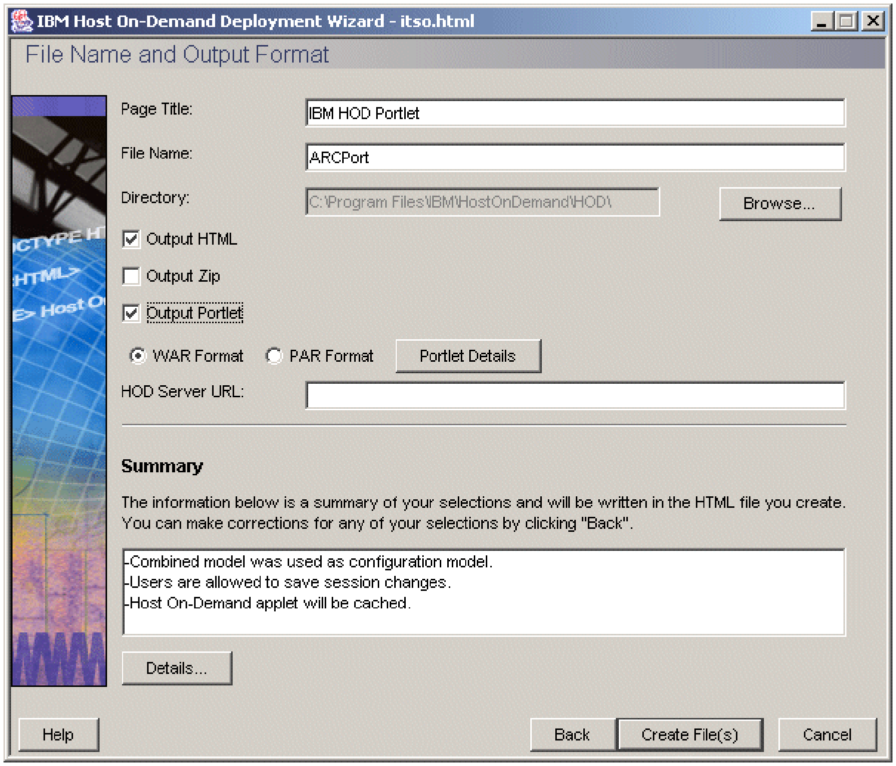
Beginning with Host On-Demand V7, the generation of portlet files became simple using the additional functions added to the Deployment Wizard. The basic use of the Deployment Wizard is explained in Chapter 14, "Deployment Wizard" on page 517. The specific options to generate a portlet file appear on the last panel of the Wizard when you are presented the options for the type of file the Deployment Wizard should generate. See Figure 19-4.

It is also possible to display a Web resource such as Host On-Demand in a portlet window by defining an inline frame using an *IFRAME* HTML tag. Further information about accessing Web content using an IFRAME tag, including a sample portlet, can be found at:

http://www.software.ibm.com/wsdd/library/techarticles/0301_konduru/konduru_0301.html

Information on the parameters supported by IFRAME can be found at:

http://www.w3.org/



File Name and Output Format

Page Title: IBM HOD Portlet

File Name: ARCPort

Directory: C:\Program Files\IBM\HostOnDemand\HOD\

☑ Output HTML

□ Output Zip

☑ Output Portlet

● WAR Format ○ PAR Format

HOD Server URL:

Summary

The information below is a summary of your selections and will be written in the HTML file you create. You can make corrections for any of your selections by clicking "Back".

-Combined model was used as configuration model.
-Users are allowed to save session changes.
-Host On-Demand applet will be cached.

Figure 19-4 Deployement Wizard portlet definition

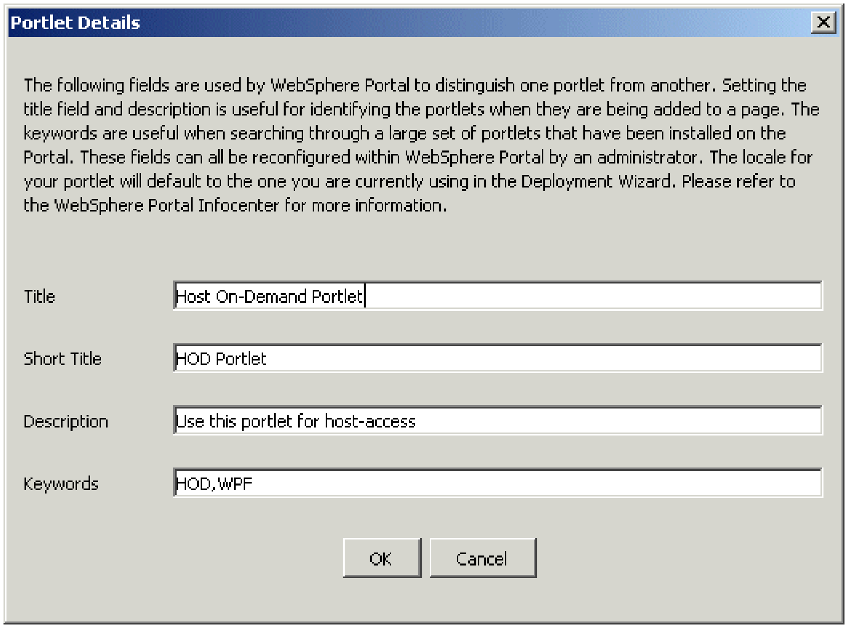
Select the type of portlet file you require:

WAR Web Archive file for WebSphere Portal V4.1 and later

PAR Portlet Archive file for WebSphere Portal V2.1 or earlier

> **Note:** The type of portlet file you generate is determined by the level of WebSphere Portal Server you are running. The different file types are *not* interchangeable.

Select the **Portlet Details** button in order to set description fields for the portlet. See Figure 19-5.



The following fields are used by WebSphere Portal to distinguish one portlet from another. Setting the title field and description is useful for identifying the portlets when they are being added to a page. The keywords are useful when searching through a large set of portlets that have been installed on the Portal. These fields can all be reconfigured within WebSphere Portal by an administrator. The locale for your portlet will default to the one you are currently using in the Deployment Wizard. Please refer to the WebSphere Portal Infocenter for more information.

Title: Host On-Demand Portlet

Short Title: HOD Portlet

Description: Use this portlet for host-access

Keywords: HOD,WPF

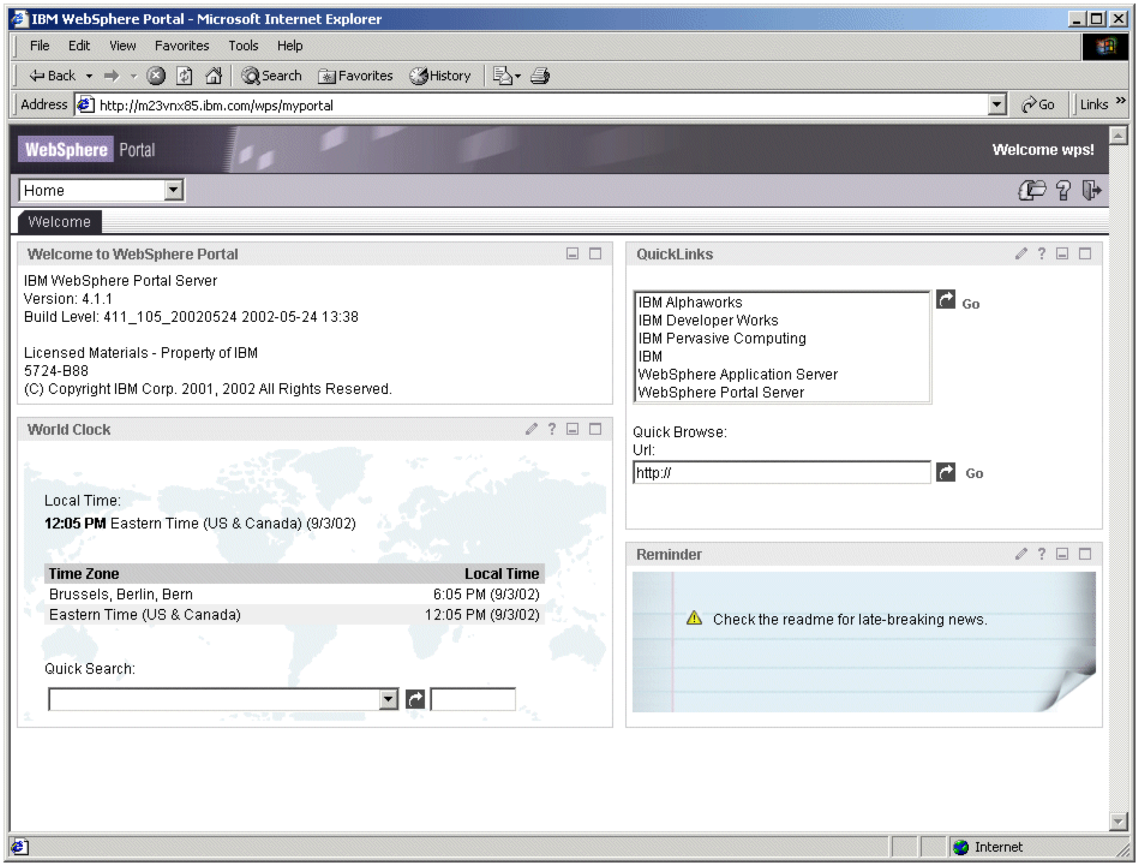
Figure 19-5 Portlet description fields

19.5 Installing the Host On-Demand portlet

In this section, we describe the process of installing a Host On-Demand portlet, created using the Deployment Wizard, in a WebSphere Portal V4.1 environment. We assume you have already installed WebSphere Portal V4.1 and all corequisite software (WebSphere Application Server, LDAP directory server, and so on).

Once you have generated the appropriate Host On-Demand portal file using the Deployment Wizard, you are ready to install this file on the Portal Server.

Navigate to the Web page you have set up to manage the WebSphere Portal V4.1 and log on as the portal administrator. A window similar to the one shown in Figure 19-6 will be displayed.


IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal
Go Links
WebSphere Portal
Welcome wps!
Home
Welcome
Internet

Welcome to WebSphere Portal

IBM WebSphere Portal Server
Version: 4.1.1
Build Level: 411_105_20020524 2002-05-24 13:38

Licensed Materials - Property of IBM
5724-B88
(C) Copyright IBM Corp. 2001, 2002 All Rights Reserved.

World Clock

Local Time:
12:05 PM Eastern Time (US & Canada) (9/3/02)

Time Zone	Local Time
Brussels, Berlin, Bern	6:05 PM (9/3/02)
Eastern Time (US & Canada)	12:05 PM (9/3/02)

Quick Search:

QuickLinks

IBM Alphaworks
IBM Developer Works
IBM Pervasive Computing
IBM
WebSphere Application Server
WebSphere Portal Server

Go

Quick Browse:
Url:
http://

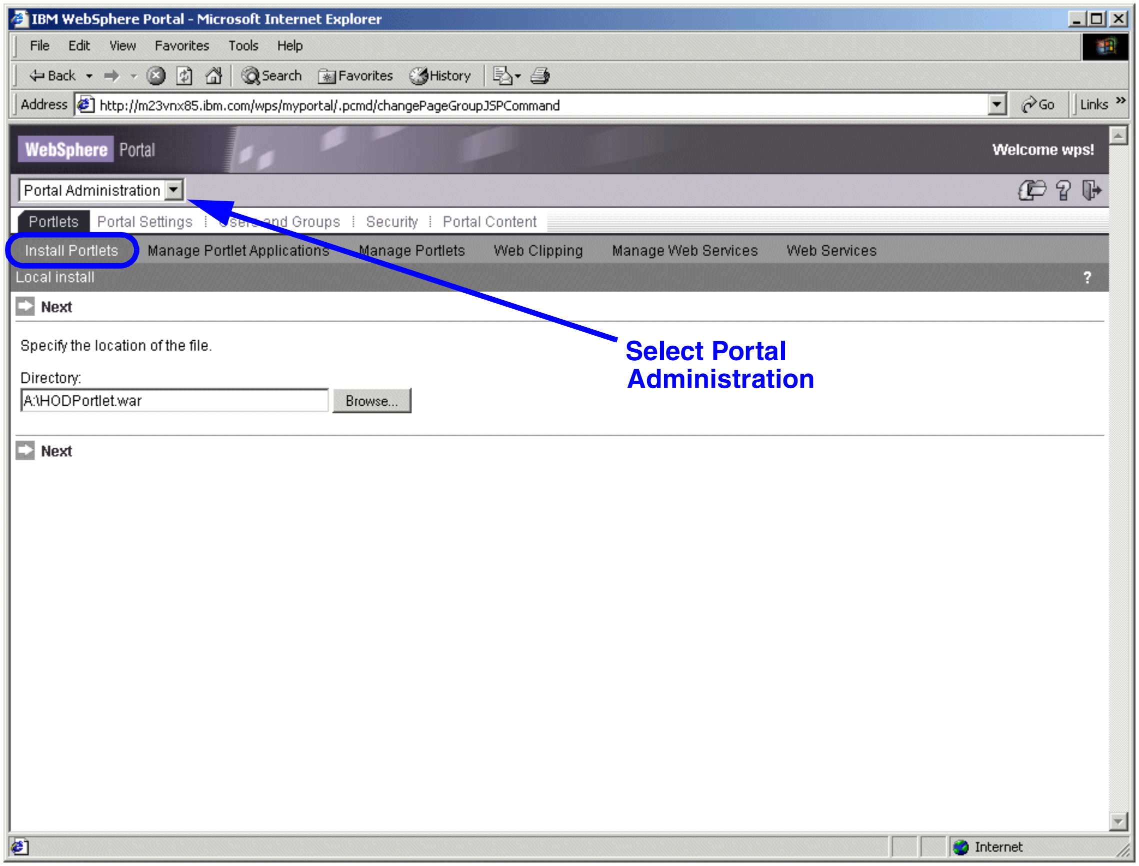
Go

Reminder

⚠ Check the readme for late-breaking news.

Figure 19-6 Portal Welcome screen after login

After you log in, select **Portal Administration** in the page pull-down on the left side of the page. See Figure 19-7.


IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.pcmd/changePageGroupJSPCommand
Go Links
WebSphere Portal
Welcome wps!
Portal Administration
Portlets
Portal Settings
Users and Groups
Security
Portal Content
Install Portlets
Manage Portlet Applications
Manage Portlets
Web Clipping
Manage Web Services
Web Services
Local install
Next
Browse...
Next
Internet
Select Portal Administration

Specify the location of the file.

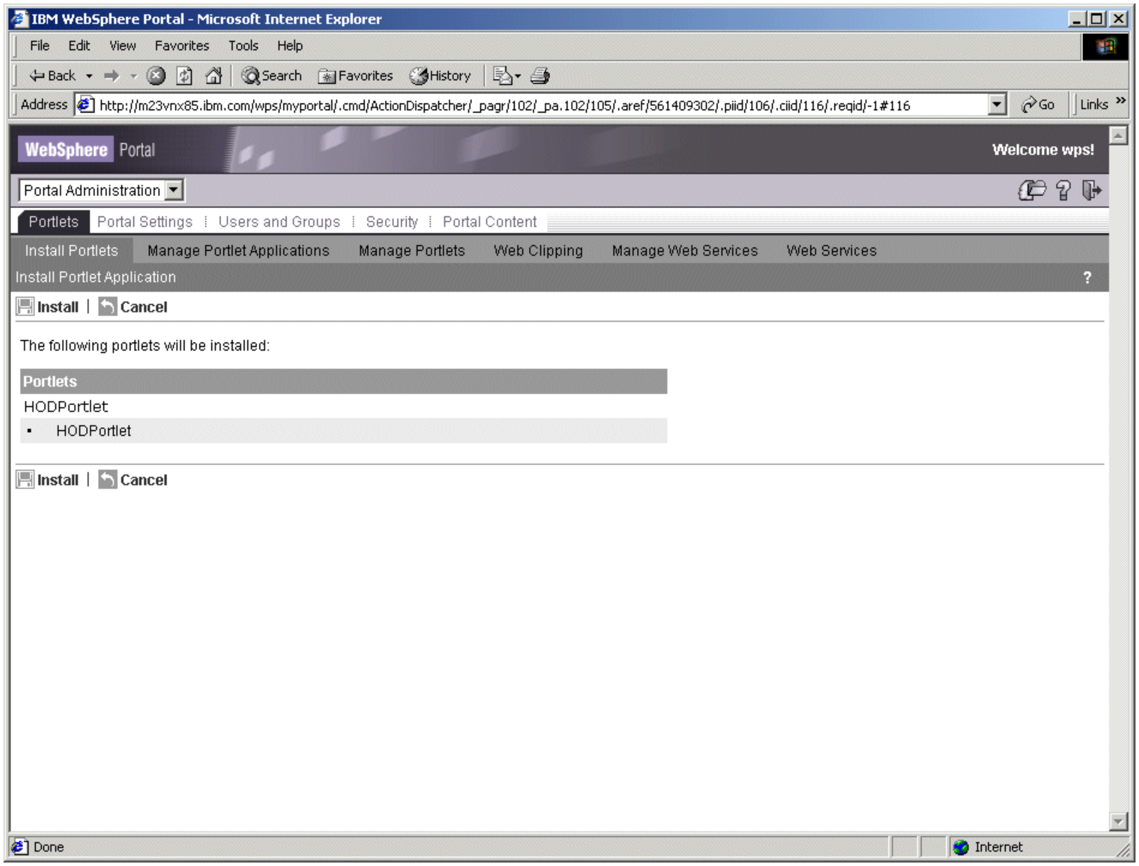
Directory: A:\HODPortlet.war

Figure 19-7 Specify location of Host On-Demand portal file

Select **Install Portlets** in the portlet menu bar.

Browse to the location of the Host On-Demand portlet file.

Install the portlet file as shown in Figure 19-8.


IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.cmd/ActionDispatcher/_pagr/102/_pa.102/105/.aref/561409302/.piid/106/.ciid/116/.reqid/-1#116
Go Links
WebSphere Portal
Welcome wps!
Portal Administration
Portlets Portal Settings Users and Groups Security Portal Content
Install Portlets Manage Portlet Applications Manage Portlets Web Clipping Manage Web Services Web Services
Install Portlet Application
?
Install | Cancel
Done
Internet

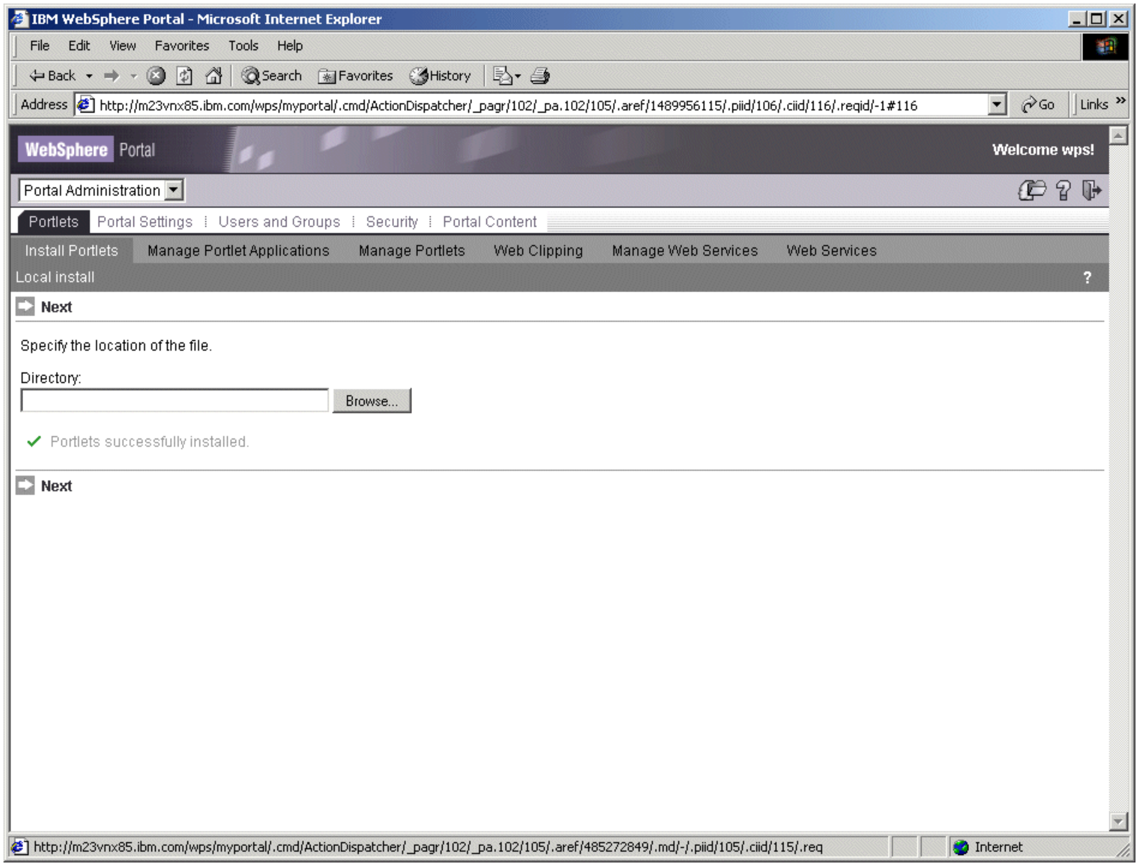
The following portlets will be installed:

Portlets
HODPortlet
• HODPortlet

Install | Cancel

Figure 19-8 List of portlets to be installed

Upon successful portlet installation, the following window will be displayed.


IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.cmd/ActionDispatcher/_pagr/102/_pa.102/105/.aref/1489956115/.piid/106/.ciid/116/.reqid/-1#116
Go Links
WebSphere Portal
Welcome wps!
Portal Administration
Portlets Portal Settings Users and Groups Security Portal Content
Install Portlets Manage Portlet Applications Manage Portlets Web Clipping Manage Web Services Web Services
Local install
Next
Browse...
Next
http://m23vnx85.ibm.com/wps/myportal/.cmd/ActionDispatcher/_pagr/102/_pa.102/105/.aref/485272849/.md/-/.piid/105/.ciid/115/.req
Internet

Specify the location of the file.

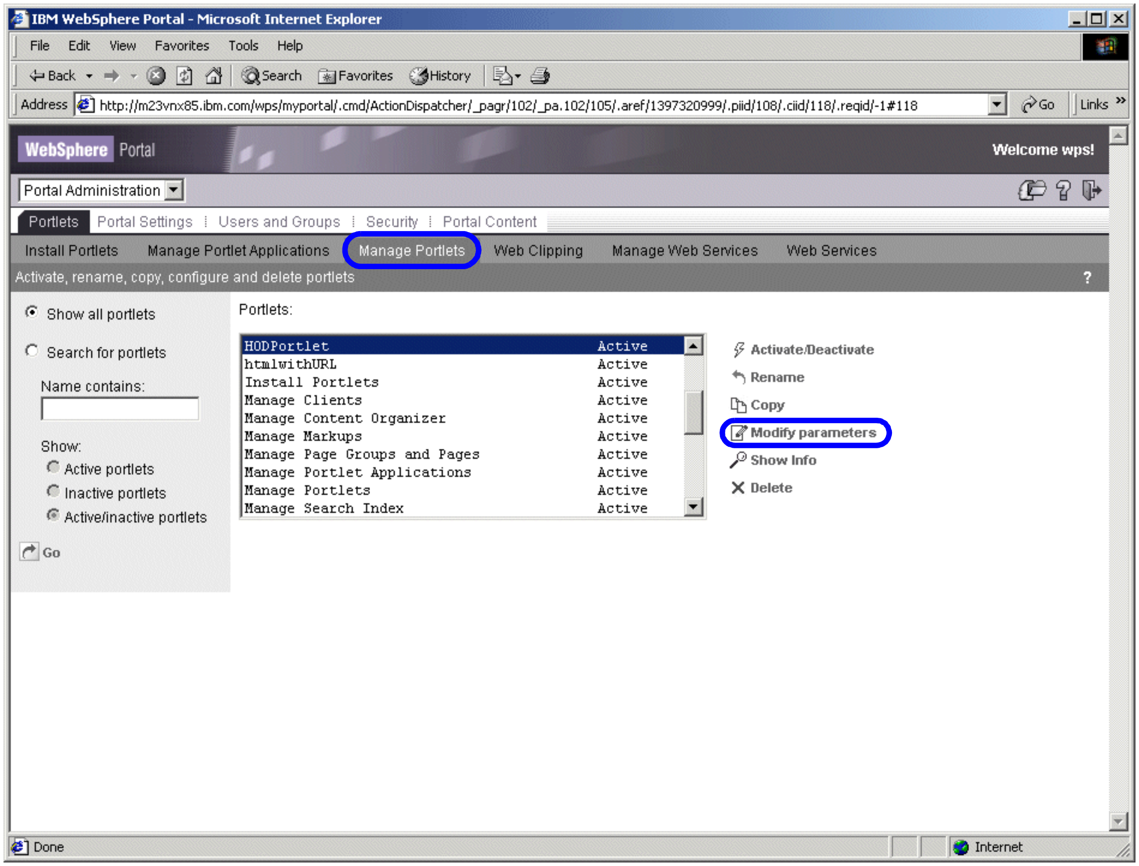
Directory:

✓ Portlets successfully installed.

Figure 19-9 Portlet install OK

After the Host On-Demand portlet is installed, you must check that it is active and ready to be deployed for use within the Portal Server.

Access the Portal Administration panel and select **Manage Portlets** as shown in Figure 19-10.

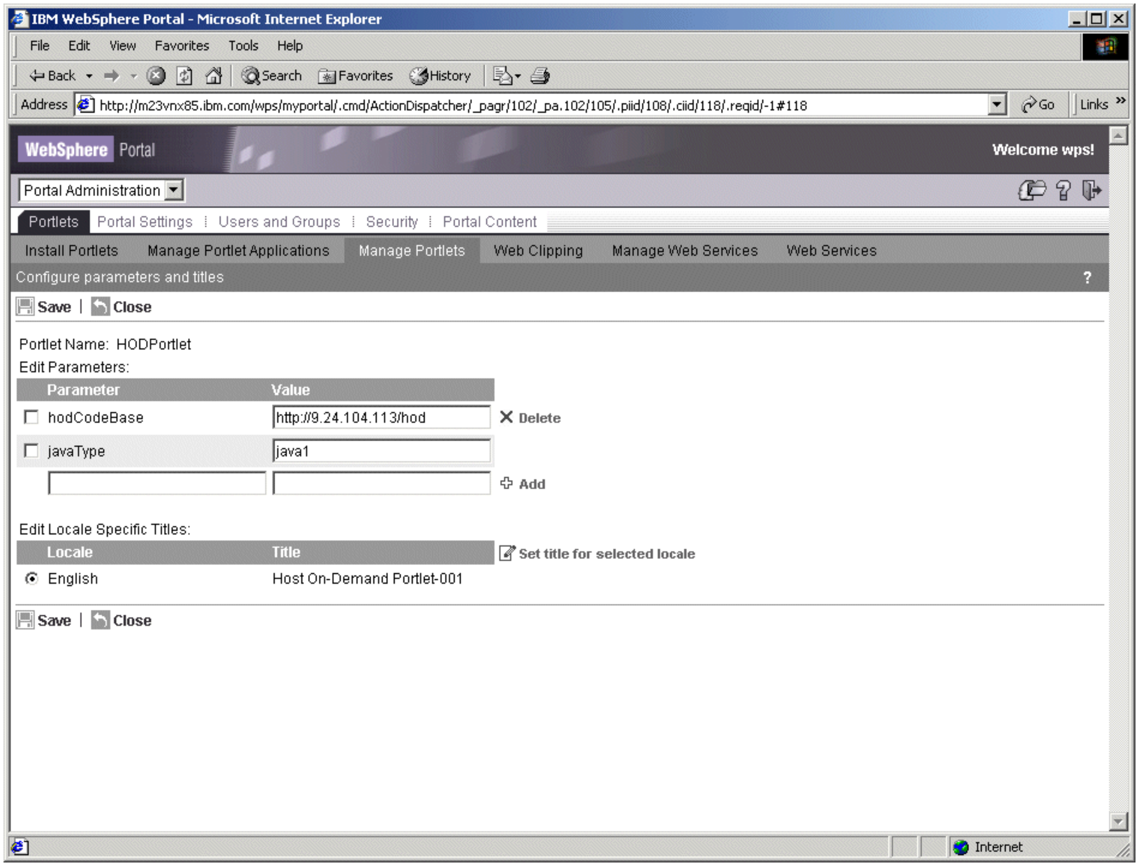

IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.cmd/ActionDispatcher/_pagr/102/_pa.102/105/.aref/1397320999/.piid/108/.ciid/118/.reqid/-1#118
Go Links
WebSphere Portal
Welcome wps!
Portal Administration
Portlets Portal Settings Users and Groups Security Portal Content
Install Portlets Manage Portlet Applications Manage Portlets Web Clipping Manage Web Services Web Services
Activate, rename, copy, configure and delete portlets
● Show all portlets
○ Search for portlets
Name contains:
Show:
○ Active portlets
○ Inactive portlets
● Active/inactive portlets
Go
Portlets:
Activate/Deactivate
Rename
Copy
Modify parameters
Show Info
Delete
Done
Internet

```
HODPortlet                         Active
htmlwithURL                        Active
Install Portlets                   Active
Manage Clients                     Active
Manage Content Organizer           Active
Manage Markups                     Active
Manage Page Groups and Pages       Active
Manage Portlet Applications        Active
Manage Portlets                    Active
Manage Search Index                Active
```

Figure 19-10 Manage portlet parameters

Verify in the displayed list of portlets that the Host On-Demand portlet you installed is active and if not, activate it.

Using the same Manage Portlet page, you can select **Modify Parameters** to update any parms originally set in the Host On-Demand portlet. This can be useful when the address for the HOD server changes, and you must modify the value for hodCodeBase as shown in Figure 19-11.


IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
WebSphere Portal
Welcome wps!
Portal Administration
Portlets | Portal Settings | Users and Groups | Security | Portal Content
Install Portlets | Manage Portlet Applications | Manage Portlets | Web Clipping | Manage Web Services | Web Services
Configure parameters and titles
?
Save | Close
Delete
Add
Set title for selected locale
Save | Close
Internet

Address: http://m23vnx85.ibm.com/wps/myportal/.cmd/ActionDispatcher/_pagr/102/_pa.102/105/.piid/108/.ciid/118/.reqid/-1#118

Portlet Name: HODPortlet

Edit Parameters:

Parameter	Value
□ hodCodeBase	http://9.24.104.113/hod
□ javaType	java1

Edit Locale Specific Titles:

Locale	Title
● English	Host On-Demand Portlet-001

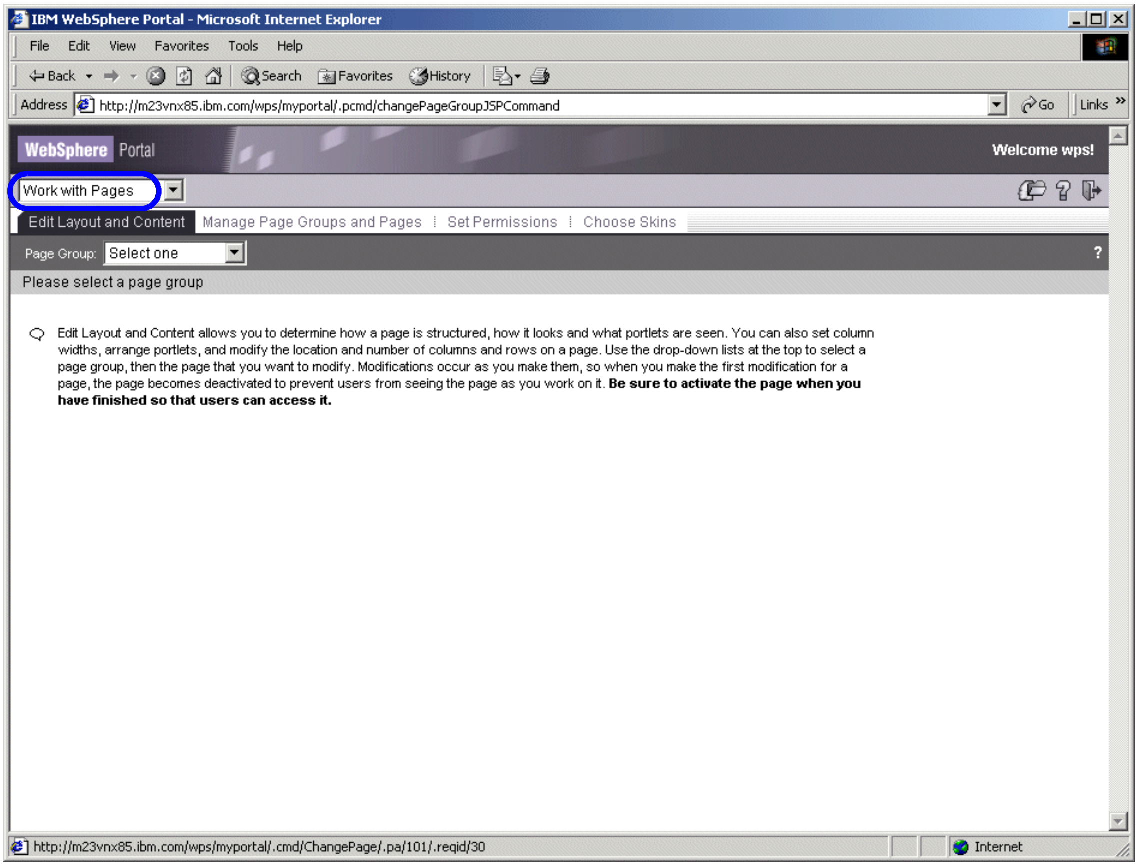
Figure 19-11 Manage portlet properties with WebSphere Portal

19.5.1 Deploying a Host On-Demand portlet to portal pages

Once you have installed the Host On-Demand portlet and made it active, you must set up individual user's pages in the Portal Server to display the Host On-Demand portlet.

Return to the Portal Server administrator console and select **Work with Pages** in the pull-down on the left side of the page. See Figure 19-12.

.

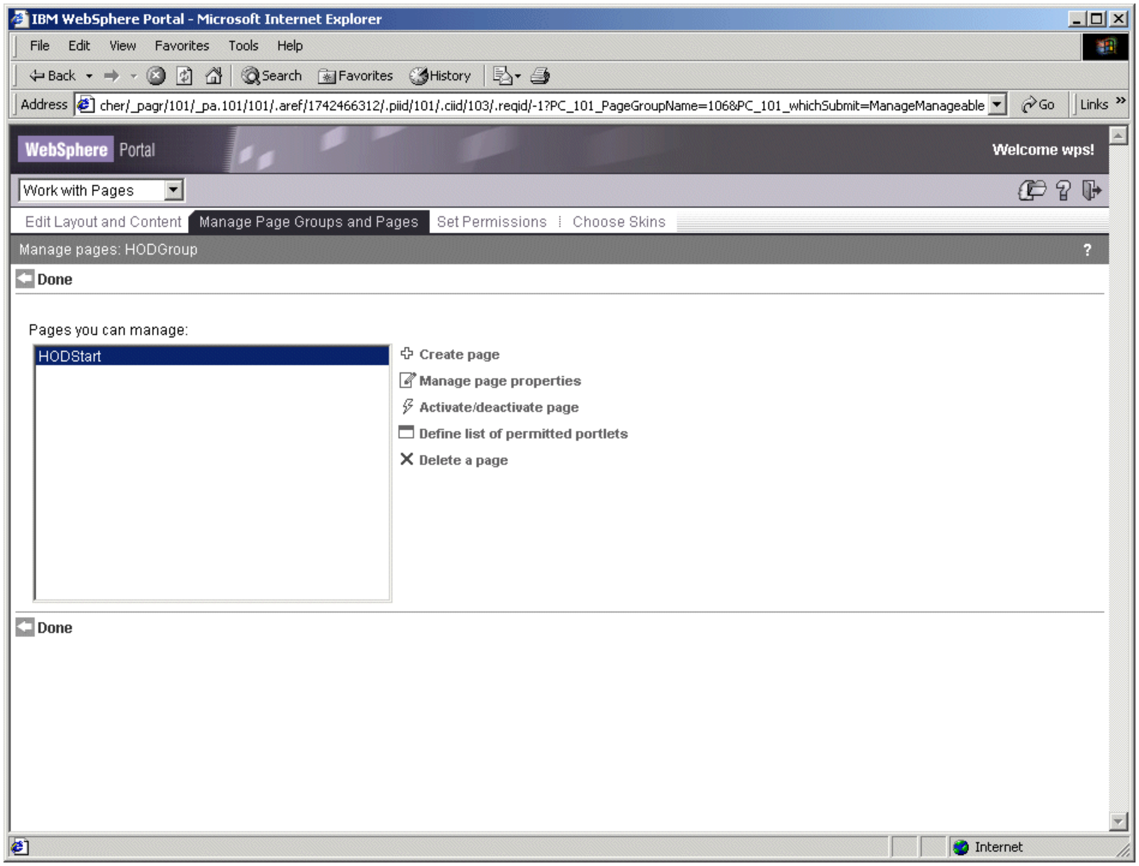

IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.pcmd/changePageGroupJSPCommand
Go Links
WebSphere Portal
Welcome wps!
Work with Pages
Edit Layout and Content
Manage Page Groups and Pages
Set Permissions
Choose Skins
Page Group: Select one
?
http://m23vnx85.ibm.com/wps/myportal/.cmd/ChangePage/.pa/101/.reqid/30
Internet

Please select a page group

Edit Layout and Content allows you to determine how a page is structured, how it looks and what portlets are seen. You can also set column widths, arrange portlets, and modify the location and number of columns and rows on a page. Use the drop-down lists at the top to select a page group, then the page that you want to modify. Modifications occur as you make them, so when you make the first modification for a page, the page becomes deactivated to prevent users from seeing the page as you work on it. **Be sure to activate the page when you have finished so that users can access it.**

Figure 19-12 Portal Server, working with portal pages

Select **Manage Page Groups and Pages** to add the Host On-Demand portlet to a user’s portal page. See Figure 19-13.



IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address cher/_pagr/101/_pa.101/101/.aref/1742466312/.piid/101/.ciid/103/.reqid/-1?PC_101_PageGroupName=106&PC_101_whichSubmit=ManageManageable
Go Links
WebSphere Portal
Welcome wps!
Work with Pages
Edit Layout and Content
Manage Page Groups and Pages
Set Permissions
Choose Skins
Internet

Manage pages: HODGroup

Done

Pages you can manage:

HODStart

- Create page
- Manage page properties
- Activate/deactivate page
- Define list of permitted portlets
- Delete a page

Done

Figure 19-13 Manage portal pages

Once the portal is deployed on a page, the users will see windows that look similar to the following figures based on the Deployment Wizard model type chosen.

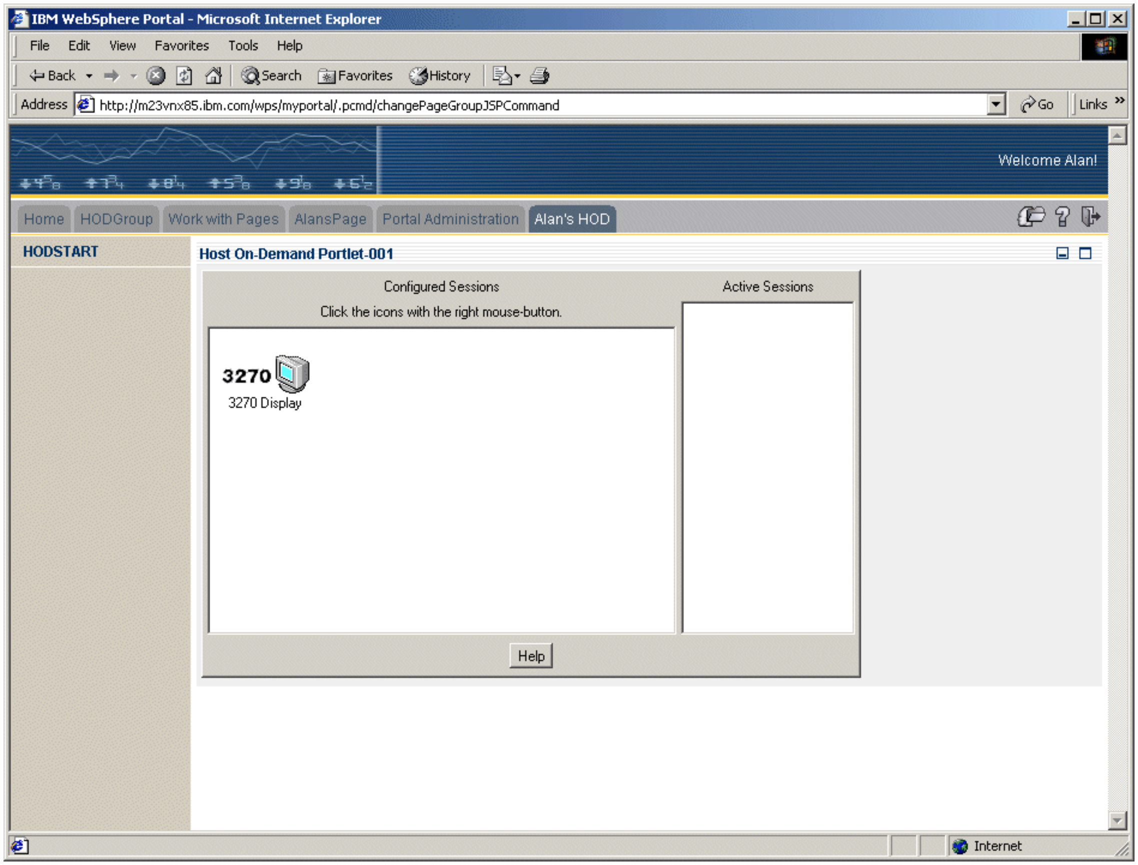

IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.pcmd/changePageGroupJSPCommand
Go Links
Welcome Alan!
Home HODGroup Work with Pages AlansPage Portal Administration Alan's HOD
HODSTART
Host On-Demand Portlet-001
Configured Sessions
Click the icons with the right mouse-button.
Active Sessions
3270
3270 Display
Help
Internet

Figure 19-14 Initial HOD portlet screen when configured to use HTML model

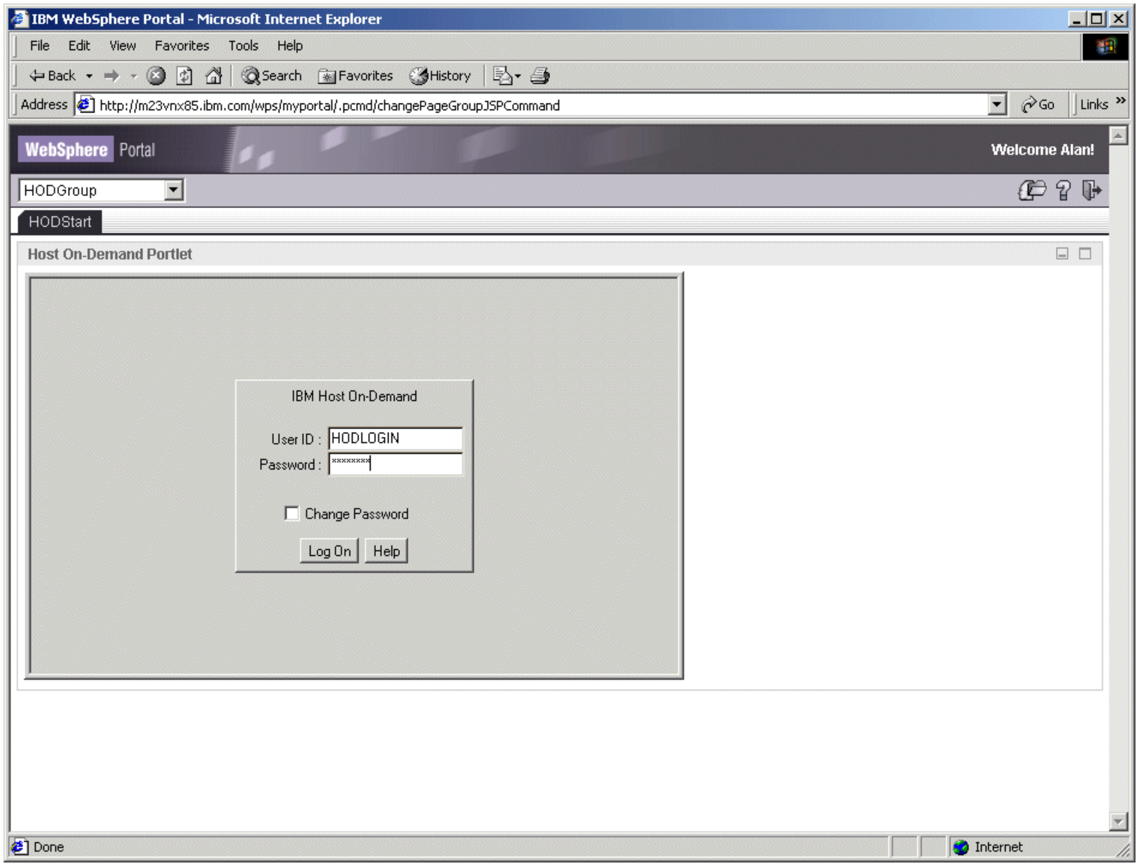

IBM WebSphere Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://m23vnx85.ibm.com/wps/myportal/.pcmd/changePageGroupJSPCommand
Go Links
WebSphere Portal
Welcome Alan!
HODGroup
HODStart
Host On-Demand Portlet
IBM Host On-Demand
User ID : HODLOGIN
Password : ********
□ Change Password
Log On
Help
Done
Internet

Figure 19-15 Initial HOD portlet screen when configured to use Config Server model

19.5.2 Special considerations when using HOD portlets

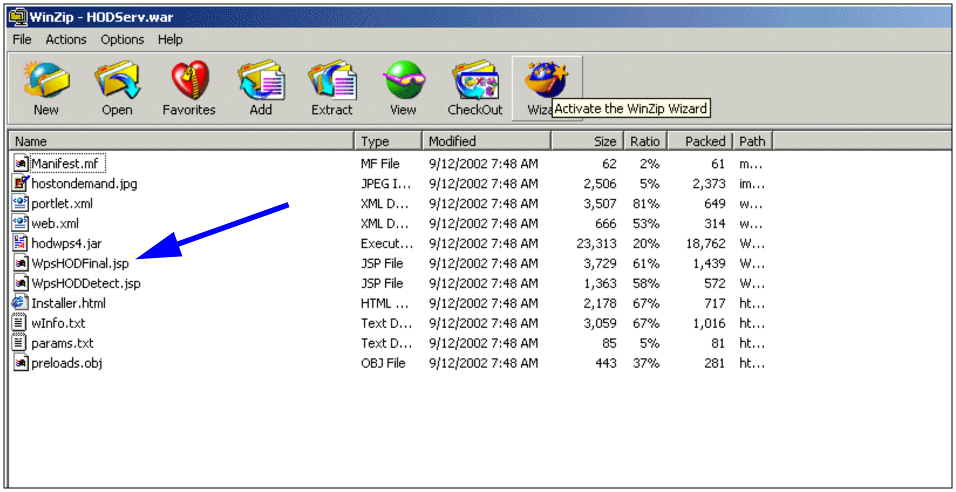
When using the Host On-Demand portlet with WebSphere Portal, the HOD administrator should consider the following issues:

1. Setting the Host On-Demand applet size for the client

   If you want an applet size that is different from the available options in the Deployment Wizard, you can modify the portlet to specify pixel width and height. To do this, you will first need to extract the portlet and locate the file called WpsHODFinal.jsp. In this file, locate the two lines beginning with var hod_AppHgt and var hod_AppWid. These are JavaScript variables defining the applet dimensions. Edit the quantities assigned to each of these variables with the dimensions you desire. Save the file, repackage the portlet, and install the portlet in your portal.

The following is an example of modifying the applet size for a portlet generated using the Deployment Wizard:

– Open the WAR file with a zip utility or the JAR utility packaged with the Java Runtime Environment. See Figure 19-16.



Name	Type	Modified	Size	Ratio	Packed	Path
Manifest.mf	MF File	9/12/2002 7:48 AM	62	2%	61	m...
hostondemand.jpg	JPEG I...	9/12/2002 7:48 AM	2,506	5%	2,373	im...
portlet.xml	XML D...	9/12/2002 7:48 AM	3,507	81%	649	w...
web.xml	XML D...	9/12/2002 7:48 AM	666	53%	314	w...
hodwps4.jar	Execut...	9/12/2002 7:48 AM	23,313	20%	18,762	W...
WpsHODFinal.jsp	JSP File	9/12/2002 7:48 AM	3,729	61%	1,439	W...
WpsHODDetect.jsp	JSP File	9/12/2002 7:48 AM	1,363	58%	572	W...
Installer.html	HTML ...	9/12/2002 7:48 AM	2,178	67%	717	ht...
wInfo.txt	Text D...	9/12/2002 7:48 AM	3,059	67%	1,016	ht...
params.txt	Text D...	9/12/2002 7:48 AM	85	5%	81	ht...
preloads.obj	OBJ File	9/12/2002 7:48 AM	443	37%	281	ht...

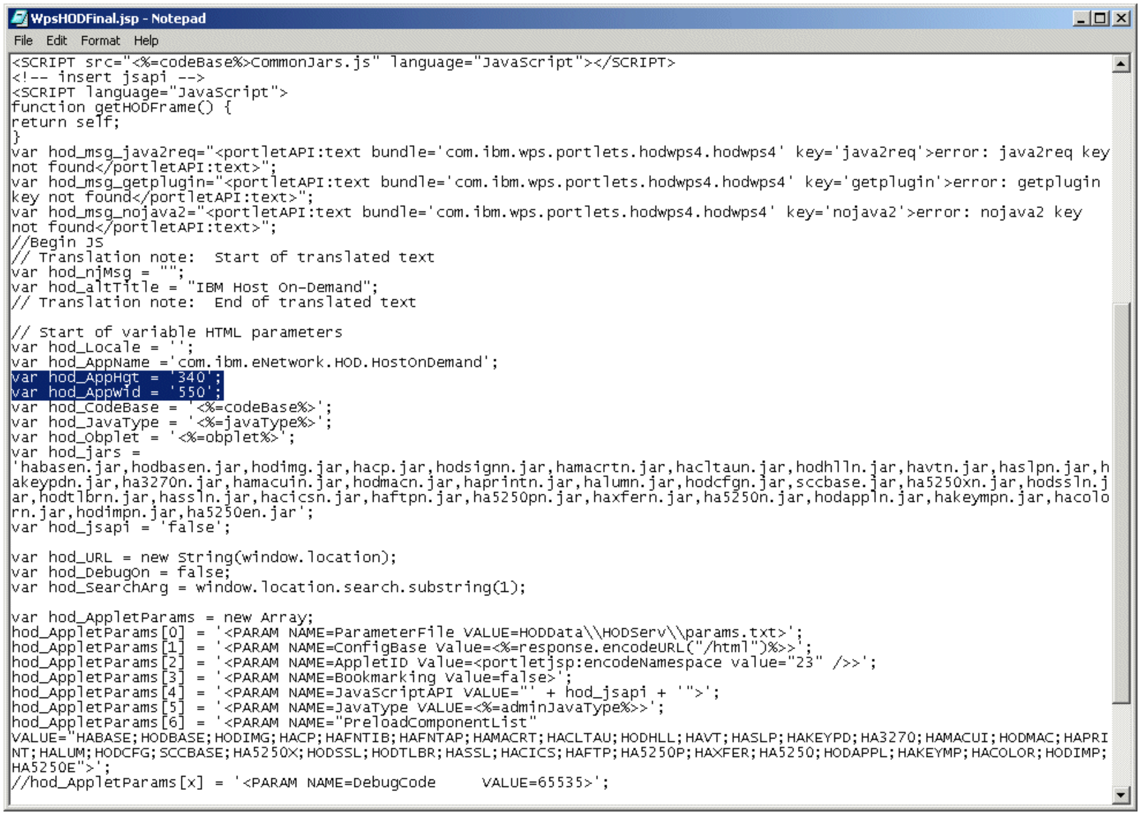
Figure 19-16 Unpack Host On-Demand WAR file

> **Tip:** The same modification of applet size can also be made for portlets defined using the *IFRAME* tag. The applet sizes are specified by modifying the height and width parameters defined in the portlet.xml file that is part of the portlet WAR file.

– Edit the file WpsHODFinal.jsp and change the values for these two variables to fit your environment, see Figure 19-17. In our example, the values of these settings are:

hod_AppHgt = '340';

hod_AppWid = '550';

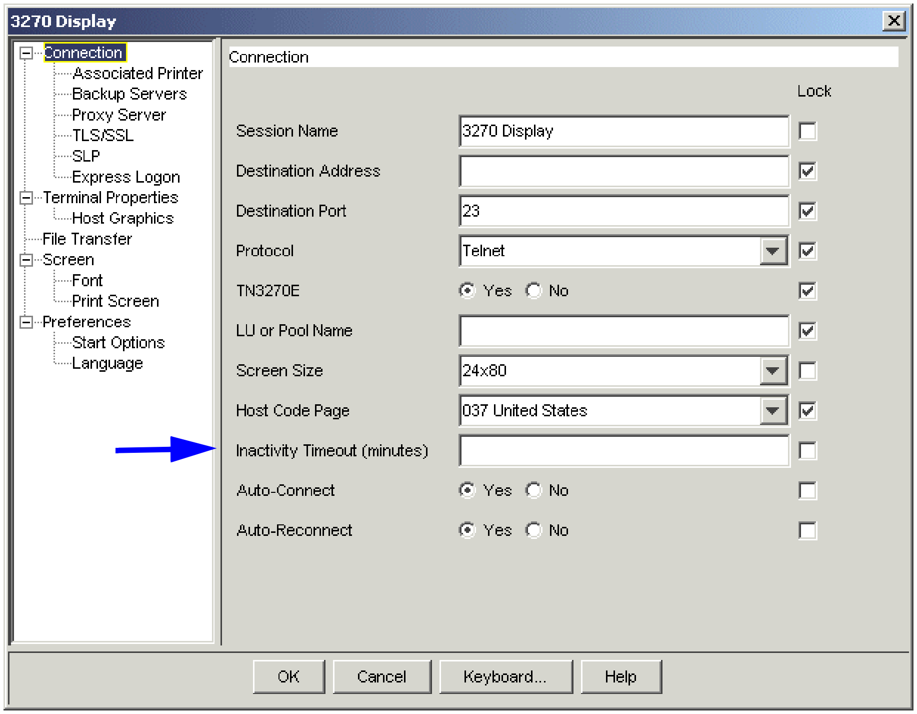


```
<SCRIPT src="<%=codeBase%>CommonJars.js" language="JavaScript"></SCRIPT>
<!-- insert jsapi -->
<SCRIPT language="JavaScript">
function getHODFrame() {
return self;
}
var hod_msg_java2req="<portletAPI:text bundle='com.ibm.wps.portlets.hodwps4.hodwps4' key='java2req'>error: java2req key
not found</portletAPI:text>";
var hod_msg_getplugin="<portletAPI:text bundle='com.ibm.wps.portlets.hodwps4.hodwps4' key='getplugin'>error: getplugin
key not found</portletAPI:text>";
var hod_msg_nojava2="<portletAPI:text bundle='com.ibm.wps.portlets.hodwps4.hodwps4' key='nojava2'>error: nojava2 key
not found</portletAPI:text>";
//Begin JS
// Translation note:  Start of translated text
var hod_njMsg = "";
var hod_altTitle = "IBM Host On-Demand";
// Translation note:  End of translated text

// Start of variable HTML parameters
var hod_Locale = '';
var hod_AppName ='com.ibm.eNetwork.HOD.HostOnDemand';
var hod_AppHgt = '340';
var hod_AppWid = '550';
var hod_CodeBase = '<%=codeBase%>';
var hod_JavaType = '<%=javaType%>';
var hod_Obplet = '<%=obplet%>';
var hod_jars =
'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hodsignn.jar,hamacrtn.jar,hacltaun.jar,hodhlln.jar,havtn.jar,haslpn.jar,h
akeypdn.jar,ha3270n.jar,hamacuin.jar,hodmacn.jar,haprintn.jar,halumn.jar,hodcfgn.jar,sccbase.jar,ha5250xn.jar,hodssln.j
ar,hodtlbrn.jar,hassln.jar,hacicsn.jar,haftpn.jar,ha5250pn.jar,haxfern.jar,ha5250n.jar,hodappln.jar,hakeympn.jar,hacolo
rn.jar,hodimpn.jar,ha5250en.jar';
var hod_jsapi = 'false';

var hod_URL = new String(window.location);
var hod_DebugOn = false;
var hod_SearchArg = window.location.search.substring(1);

var hod_AppletParams = new Array;
hod_AppletParams[0] = '<PARAM NAME=ParameterFile VALUE=HODData\\HODServ\\params.txt>';
hod_AppletParams[1] = '<PARAM NAME=ConfigBase Value=<%=response.encodeURL("/html")%>>';
hod_AppletParams[2] = '<PARAM NAME=AppletID Value=<portletjsp:encodeNamespace value="23" />>';
hod_AppletParams[3] = '<PARAM NAME=Bookmarking Value=false>';
hod_AppletParams[4] = '<PARAM NAME=JavaScriptAPI VALUE="' + hod_jsapi + '">';
hod_AppletParams[5] = '<PARAM NAME=JavaType VALUE=<%=adminJavaType%>>';
hod_AppletParams[6] = '<PARAM NAME="PreloadComponentList"
VALUE="HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HAMACRT;HACLTAU;HODHLL;HAVT;HASLP;HAKEYPD;HA3270;HAMACUI;HODMAC;HAPRI
NT;HALUM;HODCFG;SCCBASE;HA5250X;HODSSL;HODTLBR;HASSL;HACICS;HAFTP;HA5250P;HAXFER;HA5250;HODAPPL;HAKEYMP;HACOLOR;HODIMP;
HA5250E">';
//hod_AppletParams[x] = '<PARAM NAME=DebugCode     VALUE=65535>';
```

Figure 19-17 Modify WpsHODFinal.jsp

2. Host On-Demand sessions when the user logs out of the Portal Server - forcing session inactivity timeout

   Host On-Demand runs as an applet on the user's machine, and therefore does not know when the user logs out of the Portal Server. If the session is running in a separate window (default), the Host On-Demand session will continue until the user either closes the session or closes the browser. If the Host On-Demand session is running embedded in the Portal Server window and the user logs out of Portal Server, the session may appear to have ended, although the connection will remain until the browser window is closed. We strongly recommend that users close their browser window at the time they log out of the Portal Server. In addition, you may wish to configure a session inactivity timeout for your sessions. See Figure 19-18.



Connection

		Lock
Session Name	3270 Display	□
Destination Address		☑
Destination Port	23	☑
Protocol	Telnet	☑
TN3270E	● Yes ○ No	☑
LU or Pool Name		☑
Screen Size	24x80	□
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)		□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 19-18 Setting Session Inactivity Timeout

3. Installing WebSphere Portal and Host On-Demand on different servers

   If you install WebSphere Portal and Host On-Demand on different servers, certain browsers, such as Netscape 6, may give you a security violation when accessing the Host On-Demand portlet. The problem occurs because some aspects of Host On-Demand functionality rely heavily on the interaction between Java (from the Host On-Demand server) and JavaScript (from WebSphere Portal), and some browsers will not allow the interaction simply because they come from different servers. One solution is to use proxying to make it appear to the browser that WebSphere Portal and Host On-Demand are on the same server. The online Help describes how to set up proxing with the Apache/IBM HTTP server.

4. Caching versus no-Caching

   The default setting in the Deployment Wizard is to cache Host On-Demand on each user's machine. Many customers like this option with Host On-Demand because it effectively installs all necessary code on the user's machine, and does not require network loads each time the user accesses the HTML file or portlet. However, the caching behavior may not be familiar to many Portal Server users, and you may elect to reject the caching option. Caching also requires the user to restart the Web browser, forcing the user to disconnect from the portal.

5. Choosing the Host On-Demand server model

   The model you choose for your portlet (configuration server, HTML, or combined) will reflect where your sessions are configured, and will determine how user changes are stored. Although Host On-Demand treats portlets the same as HTML files, consider the following characteristics as you decide how to configure your portlet:

   a. **HTML model**: This model has no dependency on the Host On-Demand configuration server. If users are allowed to make updates, their changes will be stored on their local machines. These user changes will not be available if the user roams to a different machine. See Chapter 13, “Deployment strategies” on page 501.

   b. **Configuration Server model:** This model requires user access to the Host On-Demand configuration server. It allows your users to roam from one machine to another and still see any session modifications they may have made. For more info on this topic refer to Chapter 13, “Deployment strategies” on page 501.

      Using this model requires users to log in to Host On-Demand with a user ID and password. If you are considering forcing the use of a user ID and password to restrict access to HOD, rather then to associate specific user preferences with a specific HOD user ID, then It may be worth thinking if the user ID and password capabilities of the Portal Server can suffice, and this may allow you to consider using the HTML model.

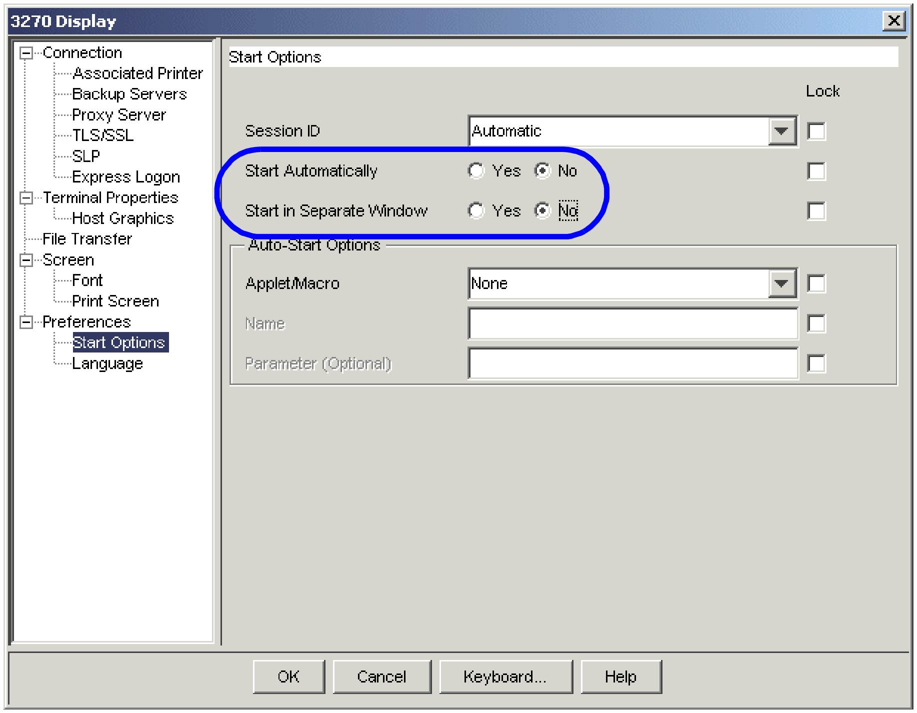
   c. **Combined model:** This model requires users to have access to the Host On-Demand configuration server in order to obtain the initial session configurations. Any user updates will be saved to the user's local machine and will not be available on a different machine if the user roams. See Chapter 13, “Deployment strategies” on page 501.

6. Starting the session automatically

   By default, Host On-Demand sessions will not start until the user selects the icon to start. If you wish to have the session start automatically, select the **Advanced** tab in Session Properties and set Start Automatically to `Yes`. See Figure 19-19.

7. Defining embedded sessions

   By default, Host On-Demand sessions are configured to launch in a separate browser window. You can choose to have the sessions launch in the same window by selecting the **Advanced** tab in Session Properties and setting Start in a Separate Window to `No`. See Figure 19-19.



Start Options

Lock

Session ID: Automatic □

Start Automatically ○ Yes ● No □

Start in Separate Window ○ Yes ● No □

Auto-Start Options

Applet/Macro: None □

Name □

Parameter (Optional) □

Figure 19-19 Embedded and auto-started sessions

8. Setting the portlet's access control in Portal Server

   The Host On-Demand portlet does not have any fields that a user can edit using the portlet interface. Therefore, when you import the portlet into Portal Server, you should set the access control to be viewable, but not editable.

19.5.3 Migrating the HOD portlet from HOD versions pre-HOD V7

There are two actions that are necessary when migrating from a pre-HOD Version 7 portlet:

- The portlet administrator must install the new portlet and make it active for all users that require it.
- The HOD administrator needs to be aware of the general client upgrade concerns. See Chapter 5, “Clients” on page 149 for more information on this topic.

19.6 Potential portlet problems

When configuring the value for HOD SERVER URL in the Deployment Wizard portlet configuration screens, you should *not* put in an address that includes an HTML file:

- Incorrect:

  ```
  //server/hod/hodmain.html
  ```

- Correct:

  ```
  //server/hod
  ```

  The trailing / is not required.

You will have errors if you code this parameter incorrectly. The errors will range from scripting errors to errors indicating portlet not running. To fix this you need to modify the hodCodeBase parameter of the portlet.

For general information on debugging WebSphere Portal, try these IBM Web sites.

WAS 2.1 troubleshooting information

InfoCenter troubleshooting information:

http://www.ibm.com/software/webservers/portal/library/InfoCenter/wps/trouble.html

WAS 4.1 troubleshooting information

- Troubleshooting:

  http://publib.boulder.ibm.com/pvc/wp/current/ena/en/InfoCenter/wps/trouble.html

- Release notes:

  http://publib.boulder.ibm.com/pvc/wp/current/exp/en/InfoCenter/wps/release_notes.html

- Portal library pages:

  http://www.ibm.com/software/webservers/portal/library.html

19.6.1 Location of portal log files

Table 19-1 Location of WebSphere Portal log files

WebSphere Portal version	**Location of Log Files**
WebSphere Portal 2.1	<Portal Home>/app/web/WEB-INF/log
WebSphere Portal 4.1	<Portal Home>/log

20

Session Manager APIs

The Host On-Demand Session Manager offers application programming interfaces (APIs) that you can use to embed host sessions in your company's Web infrastructure. Unlike the APIs included in the Host Access Toolkit, Session Manager APIs are JavaScript-based and do not require any Java programming.

Session Manager APIs are available in four different sets: Session Manager APIs, Presentation Space APIs, Host On-Demand Function APIs, and Error Reporting APIs. These APIs have many functions, including starting, stopping, and displaying either one or multiple sessions, starting macros, opening a session to the host, sending a string of text to the presentation space, retrieving text plane information, setting new string values, sending data stream function keys back to the host, and returning error messages. After an interaction is complete, the JavaScript code can switch to other tasks or simply close the session. The entire operation can be done without ever showing host screens.

In this chapter, we describe the four sets of Session Manager APIs in more detail, provide information about which components support the JavaScript API environment, and then present a real-life scenario with step-by-step instructions that show you how to embed host sessions in your own Web infrastructure. Finally, we introduce you to working demonstration code available on the Redbooks Web site that you can use as an example of how to use JavaScript APIs.

For more in-depth information about each API, including the method names, parameters, and return values, refer to the *Session Manager API Reference* in the Host On-Demand InfoCenter, accessed by clicking **Start -> Programs -> IBM Host On-Demand -> InfoCenter**.

20.1 The four types of JavaScript-based APIs

Session Manager APIs are divided into four sets: Session Manager APIs, Presentation Space APIs, Host On-Demand Function APIs, and Error Reporting APIs. This section describes each set in more detail.

20.1.1 Session Manager APIs

Session Manager APIs allow you to manipulate host sessions. Specifically, you can do the following:

- Start the specified session
- Stop the currently selected session, a specified session, or all active sessions
- Connect the currently selected or specified session
- Disconnect the currently selected or specified session
- Display the currently selected or specified session in a frame

In addition, get methods are available that return a string of all active sessions as well as the session ID of the last session started using the startSession API. Session Manager APIs allow you to manage multiple instances of a session as well as multiple sessions.

20.1.2 Presentation Space APIs

Presentation space APIs allow you to interact with host sessions within the presentation space. The presentation space is a virtual screen that contains all the characters and attributes that would be seen on a traditional emulator screen. Specifically, you can do the following:

- Send a string of text characters and keystrokes to the presentation space
- Send a given text string and keystrokes to the specified session either at the current or a specified cursor position
- Send a string to the presentation space
- Send a string to the presentation space either at the current or a specified cursor position
- Retrieve text plane information from the presentation space

- Retrieve the data from the specified session at the beginning of the presentation space
- Retrieve the data from the specified session at the beginning of the specified position or coordinates until the specified number of plane positions have been copied
- Return the number of characters copied into the last getString call's returned String object
- Check whether the currently selected session is ready for interaction, such as sending keystrokes or calling other API methods
- Reset the currently selected or specified session’s locked keyboard
- Check to see if the currently selected or specified session is ready to communicate with the host
- Provide screen recognition and OIA (Operator Information Area)-uninhibited functions

Presentation space APIs support multiple instances of a session as well as multiple sessions.

20.1.3 Host On-Demand Function APIs

Host On-Demand Function APIs include running a macro in either a currently selected or a specified session. They allow users to start a macro, such as one that automatically leads to a login screen. The macro must have been predefined in the session.

20.1.4 Error Reporting APIs

The Error Reporting API returns a saved error message from the last API call. If there was an exception thrown by Host On-Demand or Java as a result of one of the Session Manager, Presentation Space, or Host On-Demand Function APIs, then a getErrorMessage method returns the exception message.

20.2 Component support for Session Manager APIs

The following Host On-Demand components support Session Manager JavaScript API environment:

- Deployment Wizard
- Cached client
- Tracing function

20.2.1 Deployment Wizard

Use the Deployment Wizard to embed Host On-Demand sessions in your Web environment. Although all three configuration models support Session Manager APIs, we recommend the HTML-based model for Web integration. If you use the configuration server-based model or the combined model, client users will have to log in using the login screen (unless the username and password are specified in the HTML), and they will have to log off using the logoff button on the Host On-Demand desktop. This is because the JavaScript APIs do not provide login and log-off functions.

On the Other tab of the Deployment Wizard's Advanced Options window, when you select **Enable Session Manager JavaScript API** as shown in Figure 20-5 on page 702, the following code is added to your HTML file:

```
<SCRIPT LANGUAGE="JavaScript" SRC="HODJSAPI.js"></SCRIPT>
```

HODJSAPI.js provides the JavaScript interface to all the Session Manager APIs, and can be found in Host On-Demand's default publish directory `HostOnDemand/HOD`.

The Deployment Wizard now provides a user parameter called HideHODDesktop that hides the Host On-Demand desktop and session tabs once an embedded session starts. You can add this parameter on the Advanced Options' Additional Parameters tab in the Deployment Wizard. See Figure 20-6 on page 703 for additional details.

Session Manager APIs do not support bookmarking of sessions due to the embedded nature of the HTML files.

20.2.2 Cached client

The Host On-Demand cached client also supports Session Manager APIs. In the Deployment Wizard, when you select both to cache the Host On-Demand applet and to enable Session Manager APIs, the cached client's loader applet loads the com.ibm.eNetwork.HOD.JSHostOnDemand applet instead of the com.ibm.eNetwork.HOD.HostOnDemand applet.

20.2.3 Tracing

The JSHostOnDemand applet provides parameters entry and exit level of tracing for all Session Manager APIs. It also traces all exceptions. In addition, you can use the ECLPS component of the Host Access Class Library to trace Presentation Space APIs. Existing Host On-Demand components can trace the Session Manager and Host On-Demand Functions APIs and debug problems.

A new HOD.JSSessionManager option_tag traces Session Manager APIs using the TraceOptions HTML parameter. You can use this tag by doing the following in your Deployment Wizard HTML file:

- Choose to include problem determination components on the **Advanced Options -> Other window**, and
- Add `TraceOptions` in the Name field and `SaveLocation=Local, OutputFile=c:\HODTrace\trace.tlg, HOD.SessionManagerAPI=3` in the Value field in the **Advanced Options -> Additional Parameters** window. (The output file can be any valid file name.)

20.3 Example customer scenario

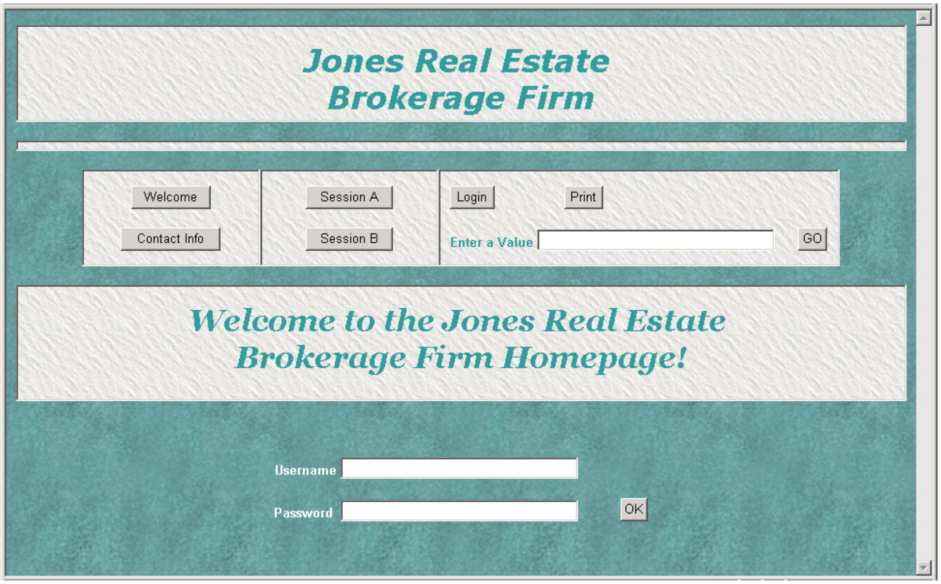
A real estate company's financial consultants access customer data through Host On-Demand sessions. The company wants to be able to embed these host sessions into its already-existing Web infrastructure, allowing its consultants to interact with the sessions and use Host On-Demand's built-in functions within the company's own personalized Web interface.

The firm is very cost-conscious and does not want to outsource Java programmers to code Java-based APIs. Instead, they prefer to use JavaScript-based APIs, which can be maintained by their own in-house Web developers.

The firm decides to take advantage of Host On-Demand's Session Manager APIs, which are JavaScript-based and are separate from the Java-based APIs provided with the Host Access Toolkit. The company's Web development team designs some Web pages that allow the company's consultants to access host sessions while maintaining the company's own look and feel. Their overall goals include the following:

- To allow single sign-on to both the company's Web server as well as host applications
- To print the contents of host sessions
- To enter values into the host sessions

Figure 20-1 shows the Web page that the company's Web development team designs for the consultants to use as a home page when they access the company's personal HTML files as well as their Host On-Demand sessions. Although the Host On-Demand sessions are active in the Web site, and the user can interact with them, the sessions are hidden in the user's browser.



Jones Real Estate Brokerage Firm

Welcome to the Jones Real Estate Brokerage Firm Homepage!

Figure 20-1 Sample home page with initial login and welcome message

Once users access the home page, the site displays a welcome message and prompts them with a login screen. After they enter their user name and password and click **OK**, they are logged into the company's Web server, and are able to access all the company's applications and Host On-Demand sessions.

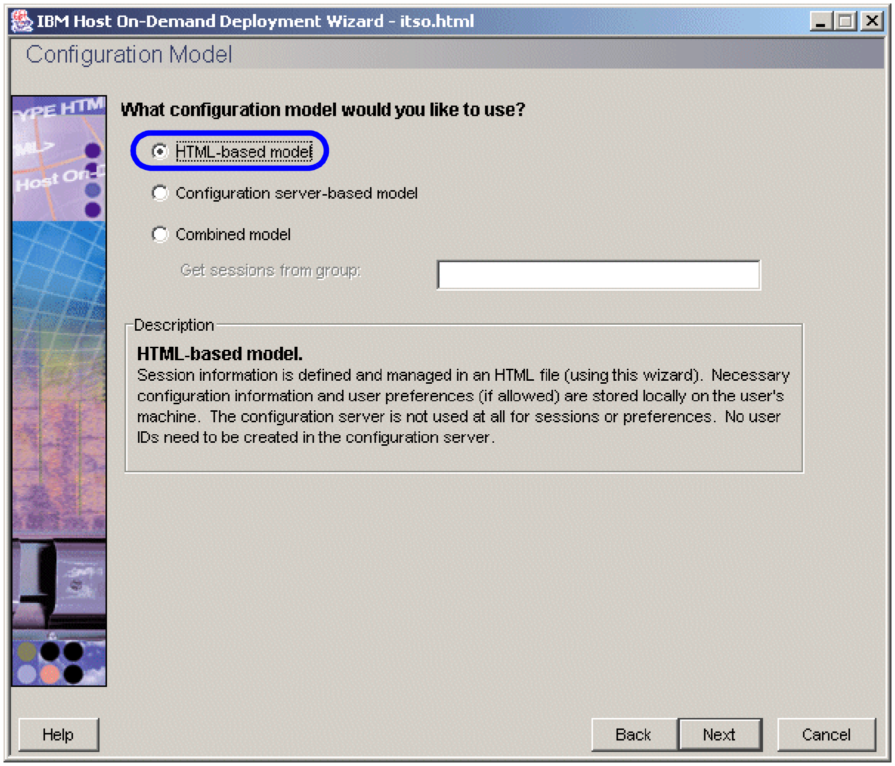
20.3.1 Instructions for embedding host sessions

Take the following steps to embed your host sessions and implement Session Manager APIs in a Web page environment similar to this example shown in Figure 20-1:

1. Use the Deployment Wizard to create your Host On-Demand HTML file or files. (In the example home page in Figure 20-1, the company has created two individual sessions using the Deployment Wizard: Session A and Session B.)

   In order to use Session Manager APIs successfully, you must perform the following steps:

   a. Select the HTML-based configuration model, as shown in Figure 20-2. Click **Next**.



IBM Host On-Demand Deployment Wizard - itso.html

Configuration Model

What configuration model would you like to use?

● HTML-based model

○ Configuration server-based model

○ Combined model

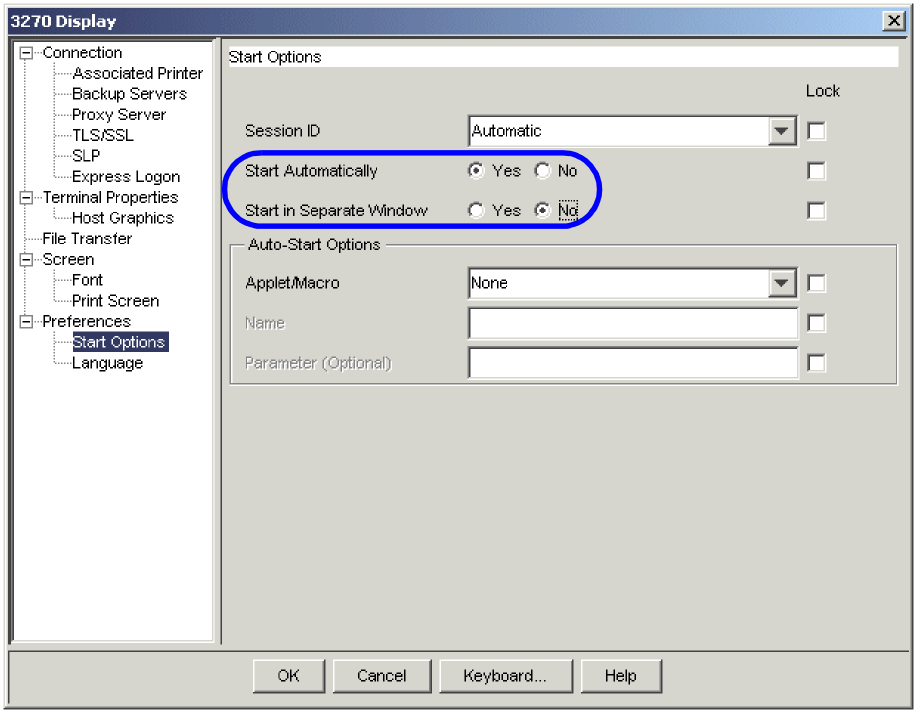
Get sessions from group:

Description

HTML-based model.
Session information is defined and managed in an HTML file (using this wizard). Necessary configuration information and user preferences (if allowed) are stored locally on the user's machine. The configuration server is not used at all for sessions or preferences. No user IDs need to be created in the configuration server.

Figure 20-2 Select configuration model

   b. Click **Configure** -> **Properties** on the Host Sessions window. On the -> **Start options** selection (Figure 20-3), set Start Automatically to `Yes`. The default setting is `No`. Also, set Start in Separate Window to `No`. The default setting is `Yes`. Click **OK**.



Start Options

Session ID: Automatic □

Start Automatically ● Yes ○ No □

Start in Separate Window ○ Yes ● No □

Auto-Start Options

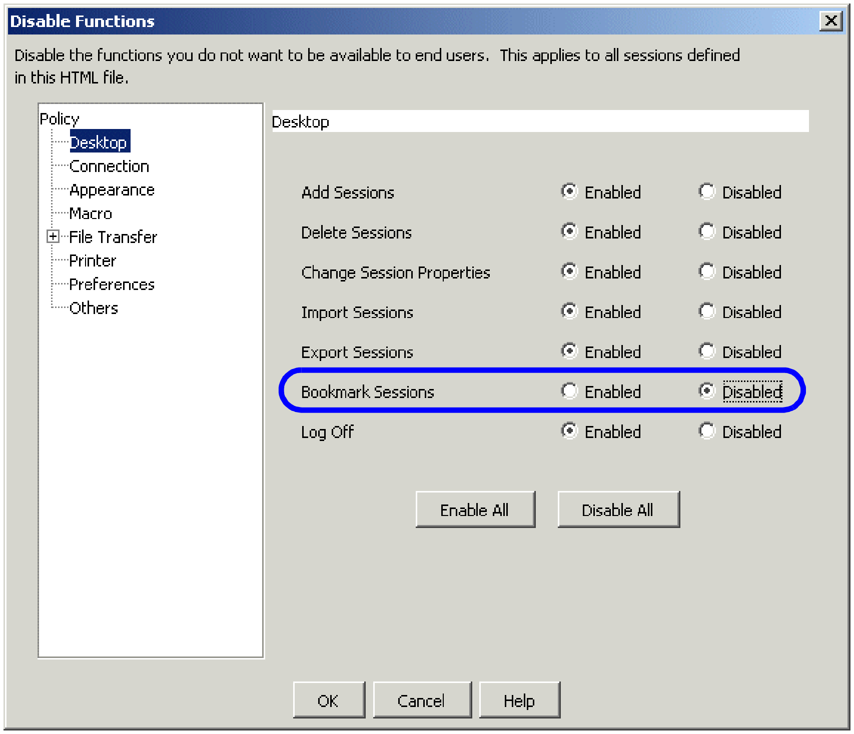
Applet/Macro: None □

Name □

Parameter (Optional) □

Figure 20-3   Start options selection

– Click **Disable Functions** on the Host Sessions window, highlight **Desktop**, and disable Bookmark Sessions (Figure 20-4). Session Manager APIs do not support bookmarking due to the frame format. The default setting for Bookmark Sessions is **Enabled**. Click **OK** and then **Next**.



Disable Functions

Disable the functions you do not want to be available to end users. This applies to all sessions defined in this HTML file.

Desktop

Add Sessions ● Enabled ○ Disabled

Delete Sessions ● Enabled ○ Disabled

Change Session Properties ● Enabled ○ Disabled

Import Sessions ● Enabled ○ Disabled

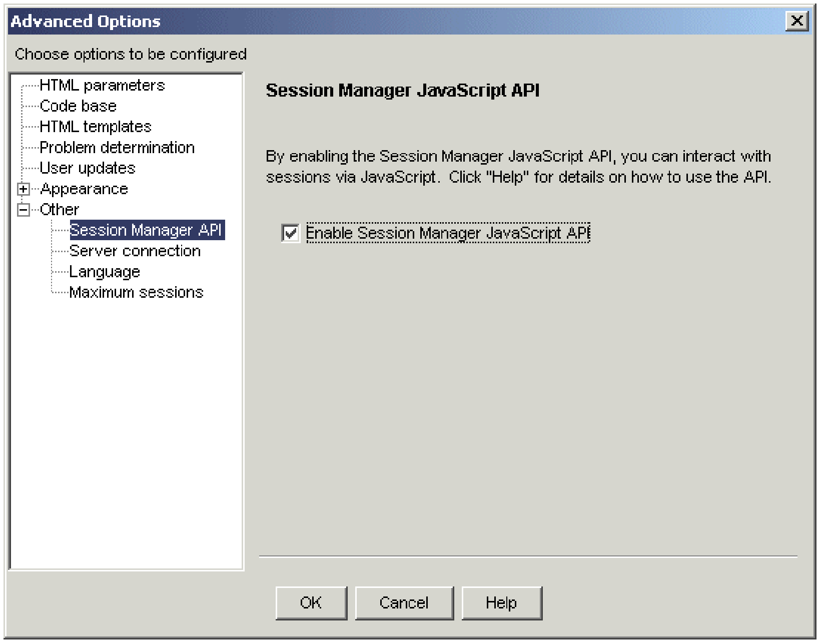
Export Sessions ● Enabled ○ Disabled

Bookmark Sessions ○ Enabled ● Disabled

Log Off ● Enabled ○ Disabled

Figure 20-4 Disable Bookmark Sessions

– In the Additional Options window, click **Advanced Options** and select **Enable Session Manager JavaScript API** on the **Other** tab, as shown in Figure 20-5. This allows a file called `HODJSAPI.js` to provide the JavaScript interface to all the Session Manager APIs. `HODJSAPI.js` can be found in Host On-Demand's default publish directory `HostOnDemand/HOD`.



Advanced Options

Choose options to be configured

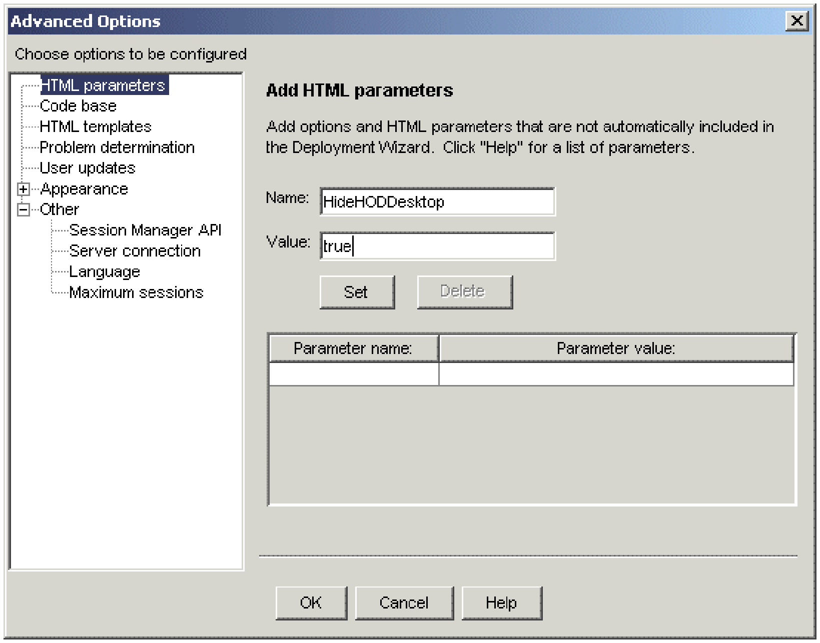
Session Manager JavaScript API

By enabling the Session Manager JavaScript API, you can interact with sessions via JavaScript. Click "Help" for details on how to use the API.

☑ Enable Session Manager JavaScript API

Figure 20-5 Session manager API selection

– On the Add HTML parameters selection of the Advanced Options window (Figure 20-6), if you want to hide the Host On-Demand desktop and session tabs once an embedded session starts, you can type `HideHODDesktop` in the parameter field and `true` in the value field. Click **Set**, **OK**, and then **Next**.



Advanced Options

Choose options to be configured

Add HTML parameters

Add options and HTML parameters that are not automatically included in the Deployment Wizard. Click "Help" for a list of parameters.

Name: HideHODDesktop

Value: true

Parameter name:	Parameter value:

Figure 20-6 Add HTML parameters selection

– In the File Name and Output Format window, create your HTML files and save it to the default publish directory, which is `/HostOnDemand/HOD`. You are now finished using the Deployment Wizard.

2. Create the main Web site (Figure 20-7) that your clients will use as a home page to access your company data. Use the following code as an example of how to divide your page into three separate frames. Notice that each frame loads a different HTML file (navigation.html, contents1.html, and Wizard_file.html).

   We have allocated 36% of the browser's frame to the first frame, 64% to the second frame, and 0% to the third frame. The reason that we did not allocate any space to the third frame is because we are hiding the Host On-Demand sessions from users. In other words, users will see only the first two frames in their browser.

Example 20-1 Pseudocode of main home page

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<TITLE>Main Home Page</TITLE>
</HEAD>
<FRAMESET rows="36%, 64%,*" frameborber="NO" name="fs">
  <FRAME src="navigation.html" name="navigation">
  <FRAME src="contents1.html" name="company_files">
  <FRAME src="Wizard_file.html" name="contentsHOD">
<NOFRAMES>
<BODY><P>To view this page, you need a browser that supports frames.</P></BODY>
</NOFRAMES>
</FRAMESET>
</HTML>
```

3. Create a file named `navigation.html`. The contents of this file are used in the first (top) frame of the home page that you created in the previous step. Use the following code as an example of how to do the following:
   - Allow the bottom frame to swap out other HTML files based on the user action in the top frame
   - Add JavaScript functions
   - Add buttons

Example 20-2 Pseudocode of navigation.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><!-- Navigation HTML file -->
<META http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<META http-equiv="Content-Style-Type" content="text/css">
<title>Navigation page</title>

<script language="JavaScript">

<!-- show me
var printBuf = " ";
var savedData = "";

//provide the swapping mecahnism
var current = 0;
var row_def = new Array("36%, 64%, *", "36%, *, 64%");
function swap(index) {
   parent.fs.rows = row_def[index];
   current = index;
}
//add the JavaScript functions
function displaySession(SessionName) {
   swap(1);
parent.contentsHOD.getHODFrame().displaySession1(SessionName);
}
function sendLoginData() {
   parent.contentsHOD.getHODFrame().sendKeys1(savedData);
}
function sendKeys(data) {
   parent.contentsHOD.getHODFrame().sendKeys1(data);
}
function setloginData(username, password) {
   saveData = username + "[tab]" + password + "[enter]";
   window.status="Saved: " + savedData;
}
function showOtherApp(pg) {
swap(0);
   parent.contents1.location = pg;
}
function printScreen() {
   printBuf = "";
   var buf = parent.contentsHOD.getHODFrame().getString();
   var row = 1;
   for (row = 0; row < 24; row ++) {
      printBuf += buf.substring(row*80, (row+1)*80) + "<br>";
}
   openPrintWindow();
}
function openPrintWindow() {
   var printWindow = window.open("JSDemoPrint.html", "PrintWindow",
"menubar,height=500,width=650");
   if(printWindow.opener == null) printWindow.opener = self;
}
</SCRIPT> //end of JavaScript
</head>

<BODY>

//add the welcome message
<div align="center"><font size="5"><i><b>Jones Real Estate Brokerage
Firm</b></i></font></div>

//create a table, add the buttons, and map the onclick parameters to the
JavaScript functions defined above

<table>
<tr>
<td><div><img src="welcome.gif" onclick="showOtherApp(‘contents1.html’);">

<td><div><img src="SessionA.gif" onclick="displaySession(‘Session
A’);"></div></td>
```

```
<td><div><img src="login.gif" onclick="sendLoginData();"></div></td>

<td><div><img src="print.gif" onclick="printScreen();"></div></td>
</tr>

<tr>
   <td><div><img src="contactInfo.gif"
     onclick="showOtherApp(‘contents2.html’);"></div></td>

   <td><div><img src="SessionB.gif" onclick=""displaySession(‘Session
      B’);"></div></td>

    <td><div><FORM name="Go">Enter a Value
    <INPUT type="text" name="SSValue" size="20">
    <IMG src="GO.gif"
       onclick="sendKeys(window.document.Go.SSValue.value+'[enter]');>
    </FORM></div></td>

</tr>
</table>

</BODY>
</html>
```

4. Create your company welcome page with the initial login. In our example in Figure 20-7 on page 708, we have created a file named contents1.html. It displays the string: `Welcome to the Jones Real Estate Brokerage Firm Homepage!` and prompts users for a user name and password when they click the **Welcome** button in the top frame. Once they enter their user name and password and click **OK**, they are logged into the company’s Web server and can access the company’s files as well as their Host On-Demand sessions.

Example 20-3 Pseudocode of contents1.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD>
<META http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<META http-equiv="Content-Style-Type" content="text/css">
<title>Welcome</title>
</HEAD>
<BODY>
<div align="center"><font size="5"><i><b>Welcome to the Jones Real Estate
Brokerage Firm Homepage!</b></i></font></div>

<FORM name="saveform"><BR>
<INPUT size="20" type="text" name="username">
<INPUT size="20" type="text" name="password">
```

```
<INPUT type="button" value="OK"
onclick="parent.navigation.setLoginData(window.document.saveform.username.value
, window.document.saveform.password.value);">
<BR>
</FORM>

</BODY>
</HTML>
```

5. Create your Contact Information page. This page will display in the bottom frame when users click **Contact Info** in the top frame. Our contact information file is named `contents2.html`.

Example 20-4 Pseudocode of contents2.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD>
<META http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<META http-equiv="Content-Style-Type" content="text/css">
<title>Contact Information</title>
</HEAD>
<BODY>
//add your company contact information here
</BODY>
```

6. Place all HTML files in your Host On-Demand publish directory. The default directory is `/HostOnDemand/HOD`.

20.3.2 Explanation of Session Manager APIs in this scenario

Now that we have taken you through the steps to create the HTML files that are used in this customer scenario, we can explain more about how this company's site makes use of Session Manager APIs.

Looking at the company’s main home page in Figure 20-7, recall that only two out of three frames are visible on the browser. The top frame displays the navigation.html file that you created in step 3. on page 704, and the bottom frame displays the contents1.html file that we discussed in step 4. on page 706.

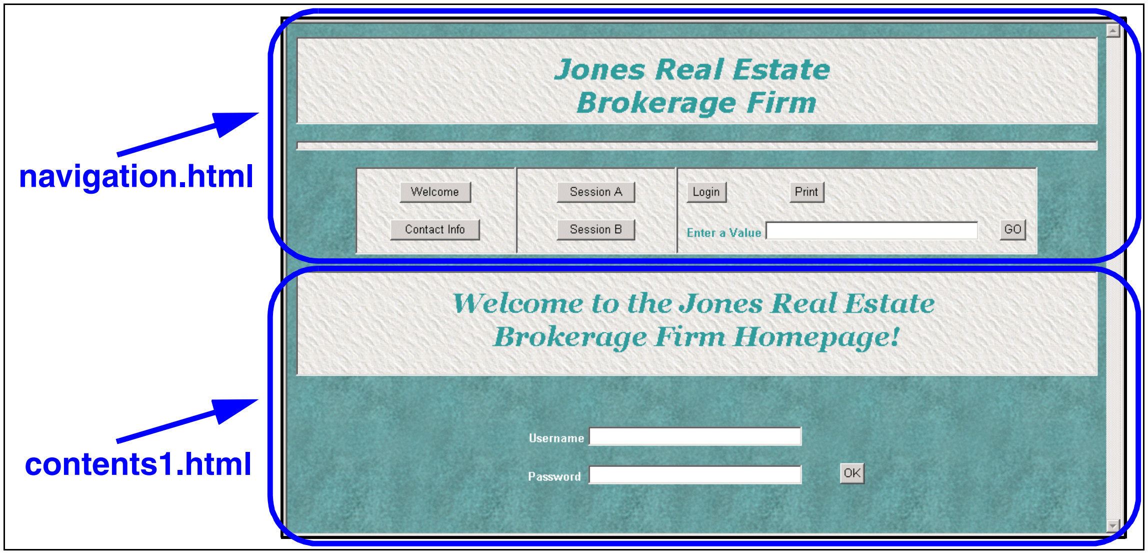
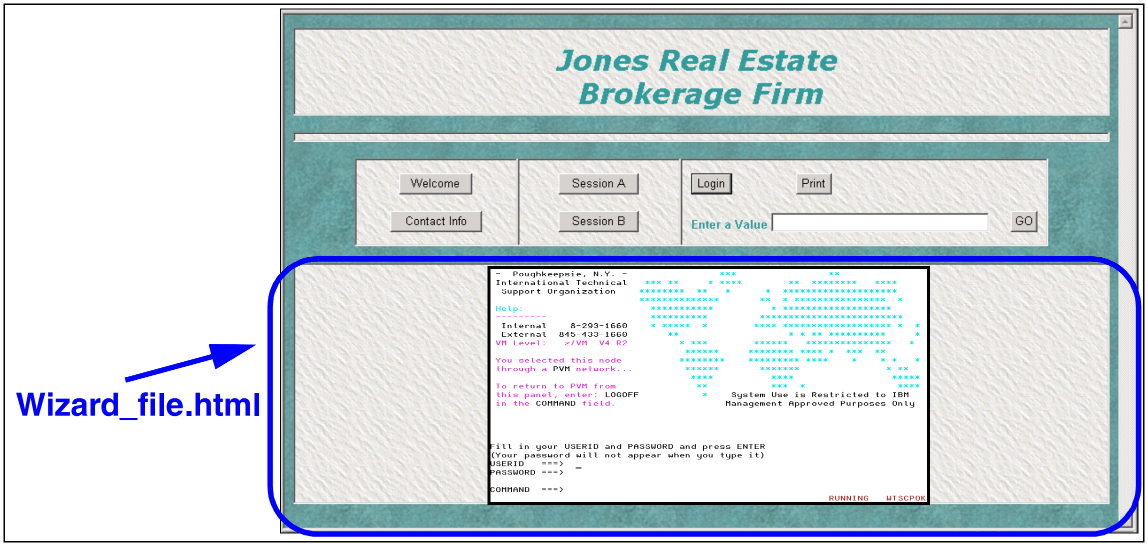


Figure 20-7 Main home page

Remember that the file you created using the Deployment Wizard (Wizard_file.html) in Step 1. on page 699 is hidden from view because we did not allocate any space to it.

The contents of the bottom frame changes depending on what the user selects in the top frame. This bottom frame can display one of two HTML files (Welcome and Contact Info) or one of two Host On-Demand sessions (Session A and Session B). For example, Figure 20-8 shows the home page after the user clicks the **Session A** button.



```
-  Poughkeepsie, N.Y. -
International Technical
 Support Organization

Help:
---------
 Internal    8-293-1660
 External  845-433-1660
VM Level:   z/VM  V4 R2

You selected this node
through a PVM network...

To return to PVM from
this panel, enter: LOGOFF            System Use is Restricted to IBM
in the COMMAND field.               Management Approved Purposes Only



Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>  _
PASSWORD ===>

COMMAND  ===>
                                                       RUNNING   WTSCPOK
```

Figure 20-8   Sample home page with Session A displayed

The Session A, Session B, Print, and Login buttons as well as the Enter a value field represent JavaScript APIs. Now we describe these built-in functions in more detail:

- When users click **Session A** or **Session B**, the displaySession JavaScript API is called to display the Host On-Demand session in the bottom JavaScript frame. Each of the session buttons will swap in one of two sessions and display the session's "green screen" as shown in Figure 20-8. Remember that the HideHODDesktop parameter was added in the Deployment Wizard file to hide the Host On-Demand desktop (see Figure 20-6 on page 703).
- When users click **Print**, the getString JavaScript API is called to retrieve the visible characters of the presentation space (called the text plane) using the TEXT_PLANE parameter. Once the API retrieves the information, the information is displayed in a pop-up window.

  The data is returned starting from the beginning of the presentation space and continuing until the JSHostOnDemand applet's buffer is full, or the entire text plane has been copied. It removes duplicate DBCS characters before the text plane data is returned.

  You can use the length variable of string object to get the number of characters copied to the returned string, or you can call the getStringLength method immediately after a getString call to get the number of characters copied to the returned string.

- When users click **Login**, the sendKeys JavaScript API is called to send the user ID and password to the current cursor position on the presentation space.

  The string consists of keystrokes that can contain text characters such as the Enter key, the Tab key, or the Page Up key. These special keys are represented by keywords that are delimited by square brackets and called mnemonics, such as `[enter]`, `[tab]`, and `[pageup]`.

  For example, in this scenario, when users first access the company's home page, the site prompts them with a login screen to access the company Web server, as shown in Figure 20-7 on page 708. Once they type the user name and password and click **OK**, the data is saved in the JavaScript code. Once they click either **Session A** or **Session B** and then **Login**, the string `userID[tab]password[enter]` is used to send the user's ID to the session screen, tab to the next field, send the user's password to the session screen, and finally execute the command. The user is now logged into the host application and is presented with the next screen.

  For a list of mnemonic keywords for the SendKeys method, and the type of session or sessions in which the mnemonic is supported, see the *Session Manager API Reference,* SC31-6355, in the Host On-Demand InfoCenter at:

  http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/hod/en/help/2tabcontents.html
- The **Enter a value** function calls the sendKeys1 JavaScript function. Similar to the Login function, the **Enter a value** function allows users to type a string of keys in the field and send this string to the current cursor position on the presentation space.

  For example, the consultants from the brokerage firm in this scenario need to enter customer information into one of the host sessions. Instead of having to navigate on the session screen and type information, the consultants can simply enter strings of keystrokes and mnemonics into the Enter a value field and click **Go**.

20.4 Description of working demonstration

Refer to Appendix E, "Additional material" on page 1065 for procedures you can follow to download the HTML code for a complete, working example using the Host On-Demand Session Manager APIs. Instructions on where to find the code, how to download it, and file names are included in the appendix. The example code must be placed in your Host On-Demand publish directory (HostOnDemand/HOD).

Similar to the real-life scenario above, the demonstration shows you working code of how to embed Host On-Demand sessions in a Web infrastructure that contains a main home page with three frames, two of which are visible in the browser. In this example, the Web developer has created three Host On-Demand sessions using the Deployment Wizard as well as two personal HTML files. Using a swapping mechanism, the bottom frame displays either one of the three host sessions, or one of the two personal HTML files at a time. The developer has also added JavaScript functions that allow the user to display, start, and stop host sessions, print the contents of the bottom frame, save data and send it to the presentation space, and play a macro.

21

Printing

Printing support in Host On-Demand V8 can be broken down into three print functions:

- Host printing: This allows host printing applications to send their print output through an LU to a printer. See 21.1, “Host printing” on page 714 for more details.
  - See 21.2, “3270 printer session” on page 719
  - See 21.3, “3270 Associated Printer Sessions” on page 735
  - See 21.4, “5250 printer session” on page 740
  - See 21.5, “3270 Host printing for DBCS” on page 745
  - See 21.6, “VT host printing” on page 748
  - See 21.7, “Adobe PDF printing” on page 749
- ZipPrint: This allows the user to generate a multi-page printout from host applications that present their output on a display, such as a file browser. See 21.9, “ZipPrint” on page 750 for more details.
- Screen copy: This allows the user to quickly print the contents of one text or graphic screen to a single page on a printer. See 21.10, “Screen copy” on page 765 for more details.

21.1 Host printing

With Host On-Demand support for host printing, you can print host-application files on a printer that is directly attached to your workstation, or to a network printer. On the host, you need a print utility that sends the data to a printer session.

This section serves as an introduction to host printing, with more detailed information being available in *IBM WebSphere Host On-Demand Version 8 Host Printing Reference,* SC31-6353, and in the online InfoCenter documentation.

21.1.1 Overview

Host On-Demand provides both a 3270 and a 5250 printer session, which runs through a browser, and uses a Java interface in the same way as a display session. Depending on the session type and platform, Host On-Demand provides three printing modes:

- Java file interface mode (3270 and 5250, all supported platforms)

  This is the printing mode used by all non-Windows platforms, and has been supported since Host On-Demand Version 3.

  In this mode, printer sessions run through a browser and use the Java File I/O API. All print data is converted into each printer's control language based on the definitions in a printer definition table (PDT) and sent to the system's printer port. As a result, printer sessions cannot use the drivers provided by the workstation's native operating system when using this mode.

  For 3270 printer sessions, the print data can be printed to file as a portable document format as used by an Acrobat reader.

- Windows spooler interface mode (3270 and 5250, Windows platforms only)

  This printing mode is supported by Host On-Demand Version 6 and later on Microsoft Windows platforms only. Like the Java file interface mode, this mode also uses a PDT to format the data, but instead of using the Java file interface, it uses the Windows native spooler interface to send the text and printer commands to the printer.

  This mode is useful when the attached printer cannot be accessed by the Java file interface, for example:

  – A USB or serial port attached printer
  – Novell NetWare network printers from Novell Windows 9x clients

- Windows native printer interface mode (3270 mode, and Windows platforms only)

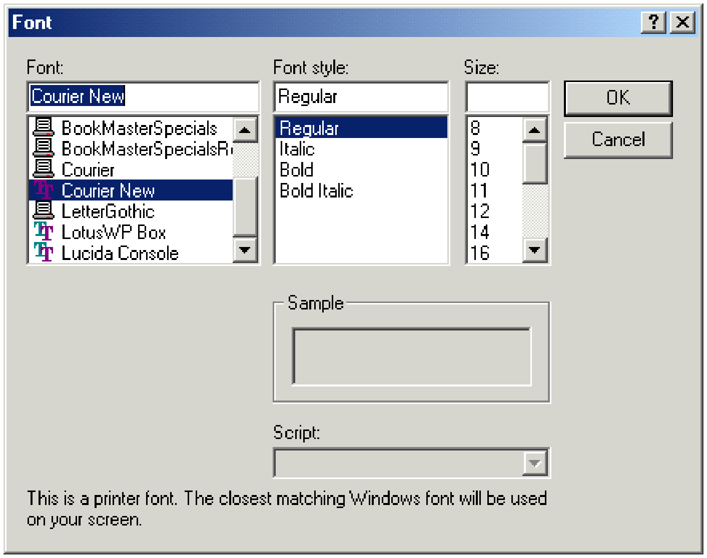
This mode formats the data more like a Windows application, using a Windows printer driver and Windows font. This mode does not require a PDT to be specified, since all formatting of the data stream is managed internally by the native printer interface.

This mode is useful when printing to a postscript printer, or when a job should be printed with a Windows font. The printer setup is well known by most users because it is the common printer setup as being used for most Windows applications.

When selecting a Windows font through the Page Setup (see Figure 21-1), the font style (regular/italic/bold) and font size are governed by Host On-Demand:

– For font style, Host On-Demand always uses “regular” except for the intensified characters on LU3 sessions. Those intensified characters are printed with the bold font.

– For font size, Host On-Demand calculates from the CPI on single-byte character set sessions. For double-byte character sets, Host On-Demand will use 10 points if the character spacing is wide enough. Otherwise, Host On-Demand calculates an appropriate point size based on the LPI and CPI values.


Font

Font: Courier New

Font style: Regular

Size:

This is a printer font. The closest matching Windows font will be used on your screen.

Figure 21-1 Selecting a Windows font

Generally, the printing modes that use a PDT (Java file interface or Windows spooler modes) will provide better performance, while the Windows native printing mode will utilize more Windows system capabilities. On non-Windows platforms, the use of a PDT is mandatory. PDTs provide great flexibility because you can tailor them to produce the desired printed output without having to modify the host application.

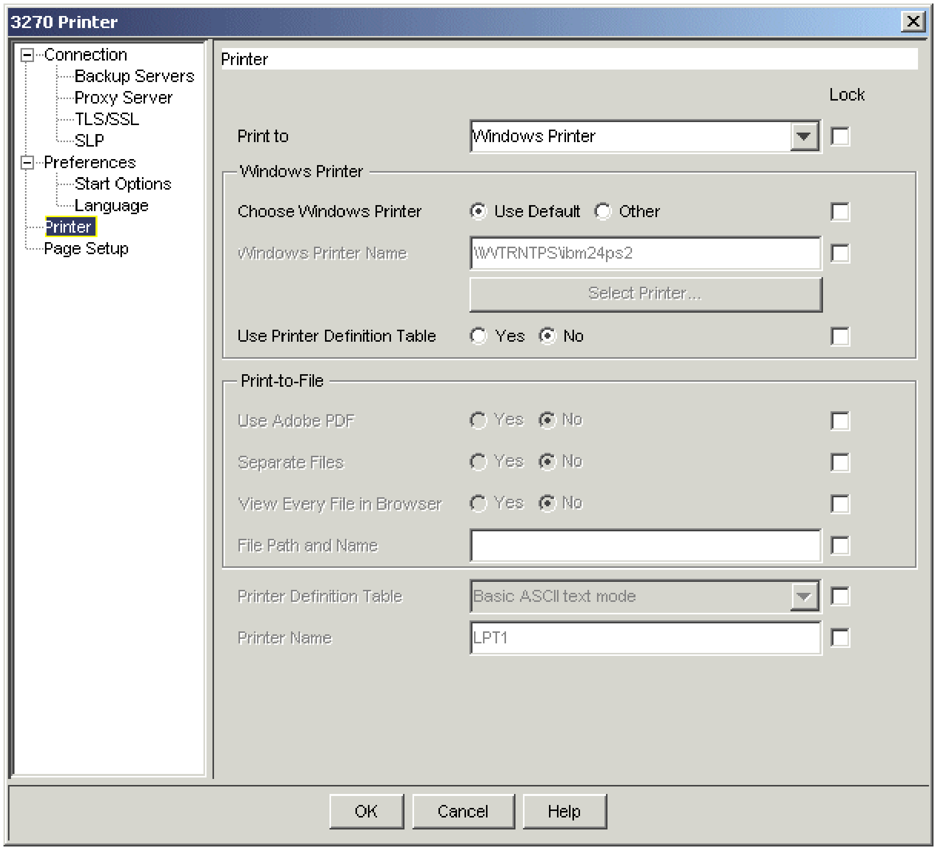
If you are using a Host On-Demand client downloaded from a server, the PDT needed for a printer session is stored on the server and downloaded with the client. A locally installed client stores the PDT on the client workstation.

Several PDTs and their equivalent Printer Definition Files (PDFs) are provided, plus you can create your own.

The following single-byte character sets (SBCS) are provided:

- Basic ASCII text mode
- HP PCL Level 3 (Laser Printers)
- IBM PPDS Level 2
- IBM PPDS Level 1 (Proprinter XL, X24, XL24)

Selections made on the Printer item (see Figure 21-2) will determine what print mode will be used.



Printer

Print to: Windows Printer □

Windows Printer

Choose Windows Printer: ● Use Default ○ Other □

Windows Printer Name: \\WTRNTPS\ibm24ps2 □

Use Printer Definition Table: ○ Yes ● No □

Print-to-File

Use Adobe PDF: ○ Yes ● No □

Separate Files: ○ Yes ● No □

View Every File in Browser: ○ Yes ● No □

File Path and Name: □

Printer Definition Table: Basic ASCII text mode □

Printer Name: LPT1 □

Figure 21-2 Printer selection on the 3270 printer session

If the Print parameter is set to:

- `Other printer`, Java interface, printing directly to printer port or to file through printer definition file or as portable document format
- `Windows Printer`, and Use Printer Definition Table is set to `No`, the Windows native printing mode is used.
- `Windows Printer` and Use Printer Definition Table is set to `Yes`, the Windows spooler interface mode is used.

21.1.2 Types of printer LU

The following information will help you decide how to configure the LU or pool name for a 3270 printer session and the Associated Printer for a 3270 display session. It also provides an explanation of the two types of printer sessions supported by Host On-Demand.

LUs are defined in different ways by various Telnet servers. To decide how to configure the Host On-Demand LU or pool name, talk to your administrator of the system programmer responsible for the server.

Explicit or implicit LU

On most servers, an LU can be defined as specific, or as a member of a pool (often referred to as *explicit* or *implicit*, respectively):

- Explicit Printer LU

  When a specific LU is configured in the Telnet server, you must enter the name of that LU in your session configuration. This ensures that the session always connects to the same LU, which is helpful for system management purposes.

- Implicit Printer LU

  When an implicit LU is configured on the Telnet server, you can either leave the LU or pool name blank, or enter the name of a pool. If you leave the name blank, the session connects to the first available LU that is defined at the server as implicit or pooled. See “LU pools” on page 719.

The LU name on the server may differ from the name of that LU at the host. Example 21-1 shows a configuration managed by a Communications Server for OS/2 server.

Example 21-1 Example configuration on Communications Server for OS/2

```
[<warpserver>-C:\]cmtn3270
                             Host     Host
Local                          Primary  Second   Idle
LU name  Class Assoc LU IP address   Status    LU       LU       mins
-------- ----- -------- ------------- --------- -------- -------- -----
@LUA0001 IW             9.24.106.179  LU-LU     ADPAVM4  X1F80202 0
@LUA0002 IW                  INACTIVE                    0
@LUA0003 IW                  INACTIVE                    0
@LUA0004 IW                  INACTIVE                    0
@LUA0005 IP             9.24.106.179  LU-LU     ADNAVEN8 X1F80206 0
@LUA0006 IW                  INACTIVE                    0
@LUA0007 IW                  INACTIVE                    0
@LUA0008 IW                  INACTIVE                    0
@LUA0009 IW                  INACTIVE                    0
@LUA000A IP                  INACTIVE                    0
```

As you can see, the LU @LUA0001 in the Communication Server gateway is connected to the host LU X1F80202 and @LUA0005 to X1F80206. Both LU names are important for printer sessions:

- The LU name in the TN3270E gateway has to be configured in the Host On-Demand printer session configuration if explicit LUs are used. It also appears in the title bar of the session window.
- Your host application has to send the print data to the LU name known at the host, for example, to X1F80206 (Class = IP means this is a printer session).

Therefore, we recommend that you give the printer LUs in the server the same names as they have at the host, so that the host LU name appears in the title bar of the printer session window, and you can see easily to which LU a print job has to be sent.

LU pools

If a group of LUs is configured in a pool at the server, the session connects to the first available LU in the pool you name. Servers handle pools in different ways, so you must configure Host On-Demand as follows:

- IBM Communications Server for Windows NT

  You can enter the name of a pool, or you can leave the LU or pool name blank if the LU desired is included in the default pool.

- IBM Communications Server for OS/2

  This does not support pools. If you want to connect to the first available LU (implicit), leave the LU or pool name blank.

- Microsoft SNA Server

  Leave the field blank.

- IBM Communications Server for AIX

  Leave the field blank, and the session will connect to the first available LU, or enter the name of a pool.

21.2 3270 printer session

A Host On-Demand 3270 printer session emulates an IBM 3287 printer in either LU Type 1 or LU Type 3 mode. The LU-type is configured at the host system, and Host On-Demand detects it automatically when the session is established. The configured LU type is significant, since some configuration parameters apply to one type or the other, and may also necessitate customization of any printer definition tables (PDT) you are using:

LU Type 1 This has an SNA Character String (SCS) data stream, which contains a series of characters, formatting commands, and attributes that can be translated from EBCDIC to ASCII and sent immediately to the printer.

Note: Only LU1 is the type of data stream which can be used with Printer Definition Files (PDF). The imbedded formatting commands can be translated by printer definition files to the appropriate escape sequence for the printer.

LU Type 3 This has a data stream that is very similar to that of a display. It is formatted by the host in a buffer, then sent to the printer.

Host On-Demand provides the following three printing modes for the 3270 printer sessions:

- Java file interface mode
- Windows spooler interface mode (Windows platforms only)
- Windows native printer interface mode (Windows platforms only)

21.2.1 Configuring a 3270 Printer Session

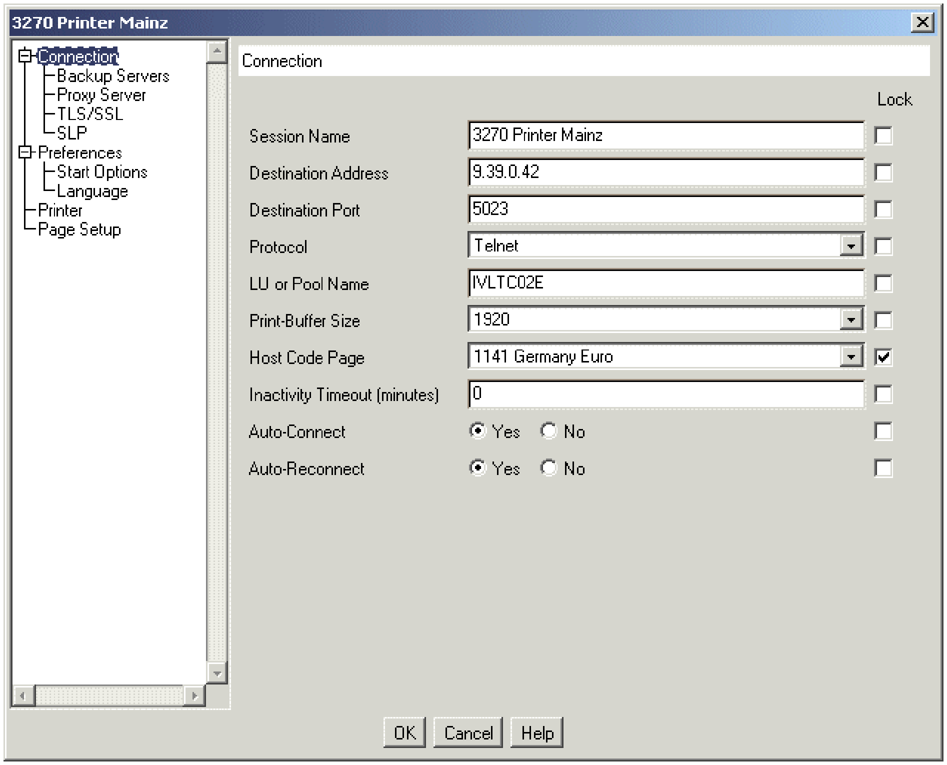
The 3270 printer session definition consists of ten selections:

- Connection
  - Backup servers
  - Proxy server
  - TLS/SSL
  - SLP
- Preferences
  - Start options
  - Language
- Printer
- Page setup

Most of these selections and their parameters (similar to the 3270 display session) are documented in “3270 and 5250 Display Sessions” on page 279. Therefore, the following paragraphs will only discuss the parameters that are specific to printing.

3270 Printer Connection selection

This selection (shown in Figure 21-3) defines the server to which the printer will connect. The only printer-specific parameter on this page is Print-Buffer Size. Select the printer buffer size that this printer session is expected to have.

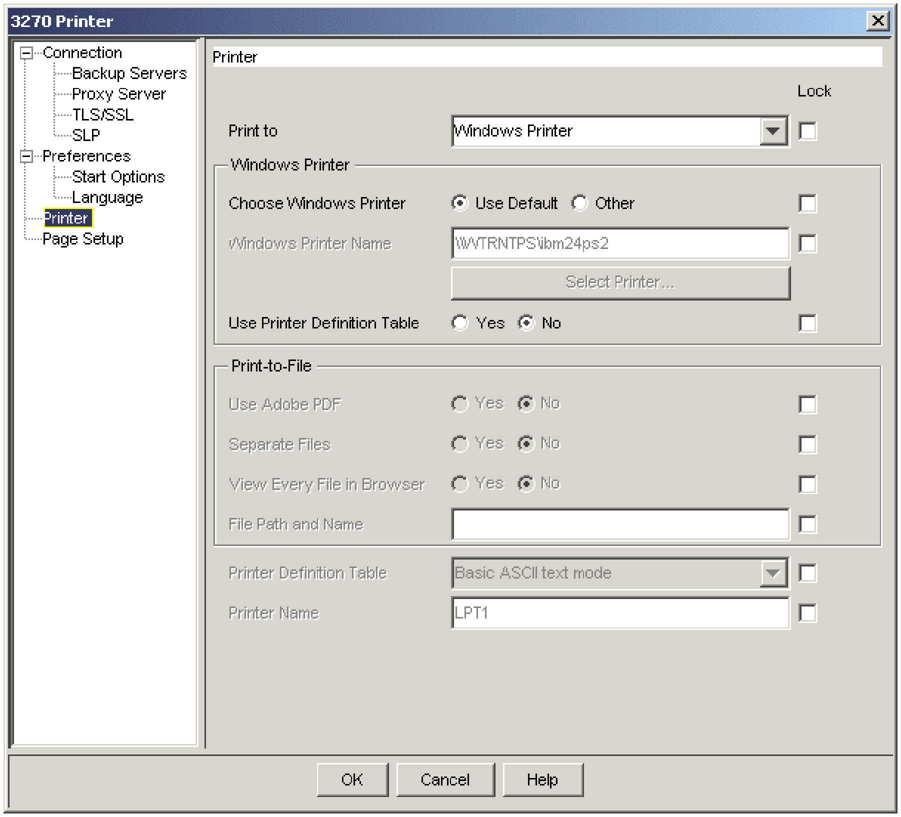


Connection

		Lock
Session Name	3270 Printer Mainz	□
Destination Address	9.39.0.42	□
Destination Port	5023	□
Protocol	Telnet	□
LU or Pool Name	IVLTC02E	□
Print-Buffer Size	1920	□
Host Code Page	1141 Germany Euro	☑
Inactivity Timeout (minutes)	0	□
Auto-Connect	● Yes ○ No	□
Auto-Reconnect	● Yes ○ No	□

Figure 21-3 3270 printer Connection selection

3270 printer Printer item



Printer

Print to: Windows Printer □

Windows Printer

Choose Windows Printer: ● Use Default ○ Other □

Windows Printer Name: \\WTRNTPS\ibm24ps2 □

Use Printer Definition Table: ○ Yes ● No □

Print-to-File

Use Adobe PDF: ○ Yes ● No □

Separate Files: ○ Yes ● No □

View Every File in Browser: ○ Yes ● No □

File Path and Name: □

Printer Definition Table: Basic ASCII text mode □

Printer Name: LPT1 □

Figure 21-4 3270 Printer item

Some of the parameters are generic for printer sessions, and are used in the 5250 printer session as well:

- Print To (3270/5250)

  Select to print to a local Windows printer (Windows platforms only), to another type of printer (for example, LPT1), or to a file. For 5250 printer sessions, printing to another type of printer requires a printer name. For 3270 printer sessions, printing to another type of printer requires a printer name and a printer definition table (PDT).

  On Windows platforms, the default is Windows Printer. On non-Windows platforms, the default is Printer.

- Windows Printer (3270/5250)

  This group box lists the options that are available only on Windows platforms:

  – Choose **Windows Printer** (3270/5250).

Select **Use Default** to use the default Windows printer. If you select **Other** then you should click the **Select Printer** button. Clicking that button opens the Windows Printer Setup dialog from which you can select from the printers defined on your system as well their settings.

  - Windows Printer Name (3270/5250)

    Displays the currently-selected Windows printer name. On Emulator clients (for example, `HOD.html`); this field is read-only. Click **Select Printer** to change the printer selection. On Administration clients (for example, `HODAdmin.html`), you can type any printer name in this field. Make sure the specified printer name is available on the client machines.

    The default value is Windows Default Printer.

  - Select **Printer (3270/5250)**

    Click this button to see the Print Setup Windows common dialog window where you can specify various settings for printing, including the printer to be used.

  - Use Printer Definition Table (3270)

    Choose whether a PDT is used or not.

    If you select **No**, the Windows graphical device interface (GDI) is used, and you can specify a printer font on the Page Setup tab.

    If you select **Yes**, the Windows spooler API is used for printing with a PDT, and you are required to specify the PDT. This selection provides better print performance over the GDI in many cases.

    The default is No.

- Print-to-File

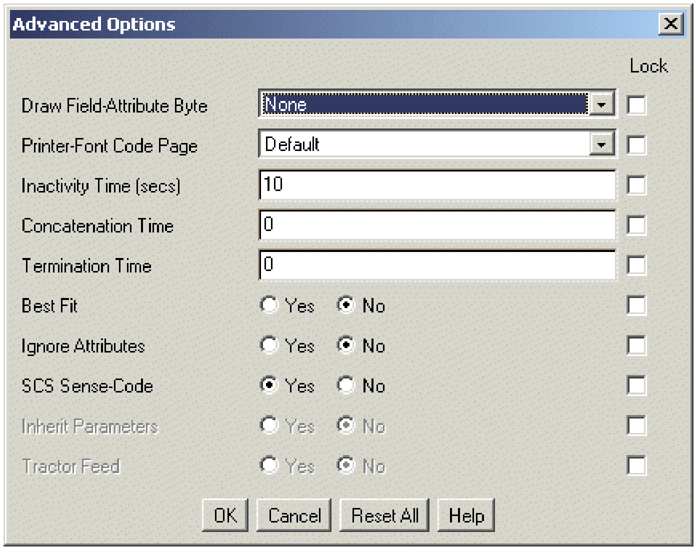
  This group box lists the options that are used for printing to a file instead of a printer.

  - Use Adobe PDF (3270)

    Select **Yes** to generate an Adobe Portable Document Format (PDF) file. This is an option only if you select to print to a file.

    The default value is No.

    If printing Adobe PDF files, make sure you have configured your requirements for PDF by going to the Page Setup selection and clicking **Advanced Options**. See Figure 21-5.



Draw Field-Attribute Byte	None	□
Printer-Font Code Page	Default	□
Inactivity Time (secs)	10	□
Concatenation Time	0	□
Termination Time	0	□
Best Fit	○ Yes ● No	□
Ignore Attributes	○ Yes ● No	□
SCS Sense-Code	● Yes ○ No	□
Inherit Parameters	○ Yes ● No	□
Tractor Feed	○ Yes ● No	□

Figure 21-5 Advanced Options window with PDF parameters

- Paper Size

  Select the paper size to be used in the generated PDF files. The default value with US English locale is “Letter.” See National Language Support for the default values when other locales are being used.

- Paper Orientation

  Select either **Portrait** or **Landscape** paper orientation. The default value is Portrait.

- Font

  Select a font from the drop-down list of predefined fonts to use in the generated PDF file. The default font with US English locale is Courier. See National Language Support for the default values when other locales are used.

  The list of fonts is also different dependent on the host code page that is currently selected. Note that the PDF file generated with the LucidaConsole font or the CourierNewPSMT font might not be displayed correctly on non-Windows or older Windows platforms. This display problem does not occur on newer Windows platforms that support OpenType fonts by default (Windows 98 Second Edition, Windows ME, Windows 2000, and Windows XP).

Some limitations for PDF printing apply (for example, limited paper size selection etc.). See 21.7, “Adobe PDF printing” on page 749 as well.

- Separate Files

  When the print destination is a file, you can choose whether you want to save each print job to a unique file, or to have jobs appended to each other in one file. When the Use Adobe PDF option is set to `Yes`, this option is not available, and each print job is saved to a unique file.

- View Every File in Browser

  Select **Yes** to view files in a browser after they are created. You can then view or print the file from your browser. If you want to view Adobe PDF files, you need to have Adobe Acrobat Reader plug-in (or equivalent) installed in your browser environment.

  Note that thumbnail images of Adobe PDF files generated by Host On-Demand do not always appear.

- File Path and Name

  When the print destination is a file, type the path and name of the file. If the file path and name already exist on the client, Host On-Demand will print the file to that destination, and will overwrite any files that already exist there. If the file path and name do not exist on the client, they are automatically created and the files will be printed to that destination. You can then view or print the file using the appropriate viewer on the client.

  Note: If you do not type the path of the file, Host On-Demand will write the file to your browser's default directory. Your browser’s default directory depends on your operating system. Refer to the *Host Printing Reference* for more information.

- If you choose **Separate = Yes** in the Separate Files field, you have a choice:

  You can specify a unique name for each file.

  Put an asterisk in the file name. The file name is numerically incriminated for each print job. For example, if you name the file prt*.file and the Use Adobe PDF option is set to `No`, the first file will be named prt000.file, the next will be named prt001.file, and so on.

  When the Use Adobe PDF option is set to `Yes`, the file extension will always set to be equal to “.pdf” and one asterisk is converted into an eight-figure counter. For example, if you name the file prt*.file, and the Use Adobe PDF option is set to `Yes`, the first file will be named prt00000001.file.pdf, the next will be named prt00000002.file.pdf, and so on.

  You can let Host On-Demand generate the name.

Do not use the asterisk in the file name. For example, type the name as prt.file. As long as the Use Adobe PDF option is set to `No`, Host On-Demand appends numbers to the file name, starting at prt.file.000, prt.file.001, and so on.

When the Use Adobe PDF option is set to `Yes`, Host On-Demand generates a file name by adding an eight-figure counter value and ".pdf" file extension. For example, when you type the name as prt.file and the Use Adobe PDF option is set to `Yes`, the first file will be named prt.file00000001.pdf, the next will be named prt.file00000002.pdf, and so on.

- If you choose **Separate = No** and the Use Adobe PDF option is set to `No`, a single file is created and each job is appended to this file. A system-generated print-job name is added to the start of each job so that jobs can be identified. If the file already exists, the system will continue to append to it.

  You can also specify an external command to run after host print jobs using this field. Refer to "Running external commands" after host print jobs in the Online Help.

  Refer to the *Host Printing Reference* for more information about Adobe PDF files, file paths, and file names.

- Printer Definition Table

  A printer definition table (PDT) formats print data sent by the host application so it can be printed on a workstation printer.

  The PDT you select must be suitable for the printer and for the printer-emulation mode that the printer will use (PCL, PPDS etc; note that PostScript is not supported). You can create your own PDTs, which are automatically added to the pull-down list (for details on PDFs see 21.11, "Changing and using PDF files" on page 769).

  Select a name from the pull-down list.

  If you are not sure which printer emulation modes are supported by your printer, you must refer to the printer's technical documentation, which usually lists the supported modes.

  In some cases, it may be necessary to change the settings on the printer itself so that they match the mode intended for the PDT that you want to use. Some printers can switch between modes automatically or supply software that enables you to change the mode. It is important to refer to the printer documentation to decide which PDT to use, and how to set the correct mode on the printer.

  You might find it useful to go to the printer manufacturer's Web site for information.

Most laser printers can use HP PCL Level 3. Level 3 commands are understood by later levels.

Basic ASCII text mode may work if your printer does not support one of the other modes supported by Host On-Demand; however, if you use this mode, the commands that are unique to your printer will not be available.

Host On-Demand does not support PostScript mode with a PDT. If you are using Host On-Demand on a Windows platform, you can use your PostScript printers as a Windows printer without a PDT.

VT sessions do not use a PDT when non-Bidi code page is being selected. Printer data from the VT application is sent as-is to the printer device. You must insure that your VT application supports the printer you want to use.

- Printer Name

  Type the name of the port for the printer you want to use. On Windows workstations, you can also type the Universal Naming Convention (UNC) name of a network printer in either of two formats:

  ```
  \\server_name\printer name
  \\server's_host_name_or_IP_address\printer name
  ```

  For example, if you are configuring a printer on Windows 95 or NT, you can type a port name such as LPT1, or a network printer name such as \\myhost\printer. If you are configuring a printer on UNIX, type a device name such as /dev/lp0.

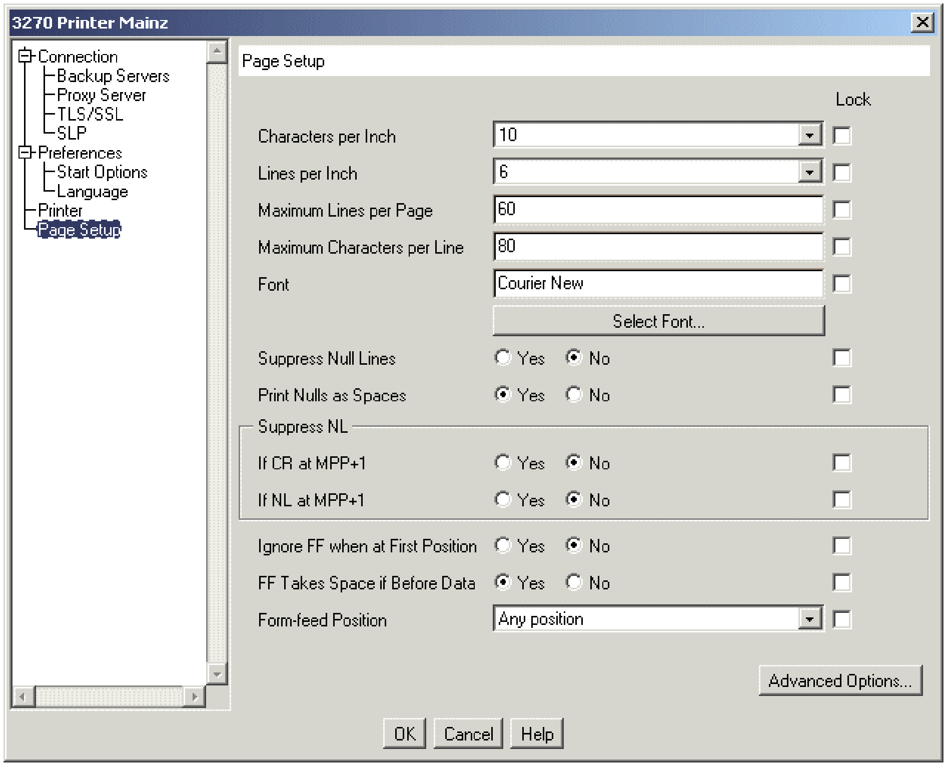
For further details and 5250 specific parameters, please refer to the online help of that selection.

3270 Page Setup item

The Page Setup item window as shown in Figure 21-6 lets you choose several options used in 3270 host print. When a PDT is being used, some values set on this panel will temporarily override the values set in the PDT. The changes are effective only for sessions started from this configuration; they do not alter the PDT. Change these options only if you are familiar with VTAM and with LU Type 1 and LU Type 3 protocols.

The values you set remain in effect for this configuration, even if your administrator later modifies and recompiles the PDT. The host SCS commands take precedence over the following when the Bestfit options were not set to `Yes` on the Advanced Options window:

- Characters per inch
- Lines per inch
- Maximum lines per page
- Maximum characters per line



Page Setup

Lock

Characters per Inch: 10 □

Lines per Inch: 6 □

Maximum Lines per Page: 60 □

Maximum Characters per Line: 80 □

Font: Courier New □

Suppress Null Lines: ○ Yes ● No □

Print Nulls as Spaces: ● Yes ○ No □

Suppress NL

If CR at MPP+1: ○ Yes ● No □

If NL at MPP+1: ○ Yes ● No □

Ignore FF when at First Position: ○ Yes ● No □

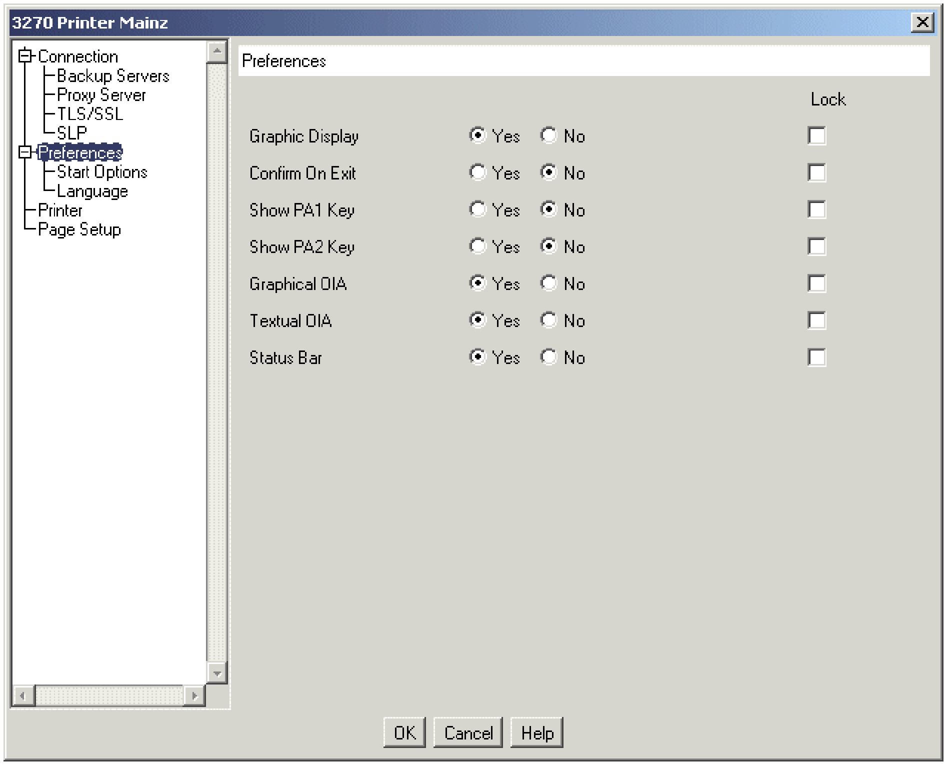
FF Takes Space if Before Data: ● Yes ○ No □

Form-feed Position: Any position □

Figure 21-6 printer Page Setup selection

3270 printer screen item

The screen item for printers controls what options the user has available on the session window representing the printer session. The controls are shown in Figure 21-7.



Preferences

			Lock
Graphic Display	● Yes	○ No	□
Confirm On Exit	○ Yes	● No	□
Show PA1 Key	○ Yes	● No	□
Show PA2 Key	○ Yes	● No	□
Graphical OIA	● Yes	○ No	□
Textual OIA	● Yes	○ No	□
Status Bar	● Yes	○ No	□

Figure 21-7 3270 printer Preferences selection

The following describes the options:

- Graphic Display

  If you turn on Graphic Display, the information window for this session will show the printer, workstation, and host system as icons. Therefore, the window will be bigger than when just displaying the raw information.

- Confirm on Exit

  Select **Yes** if you want a warning message to appear when a user attempts to close a session. If users select **File -> Exit**, close a session window, exit from the toolbar, or right-click the left corner of the session window; a window appears asking if they really want to exit. If the user clicks **OK**, the session ends. If the user clicks **Cancel** or closes the window, the session remains open and unchanged. If the user closes the browser window, no exit warnings appear. If the user closes both a session and its associated printer session, the exit warning appears only once.

The default is No.

- Show PA1 Key

  Specifies whether the Program Attention 1 key should be displayed on the window as a button.

- Show PA2 Key

  Specifies whether the Program Attention 2 key should be displayed on the window as a button

- Graphical OIA

  Determines whether the Graphical Operator Information Area (OIA) is visible on the screen

  The default is Yes (visible).

- Textual OIA

  Determines whether the Textual OIA is visible on the screen

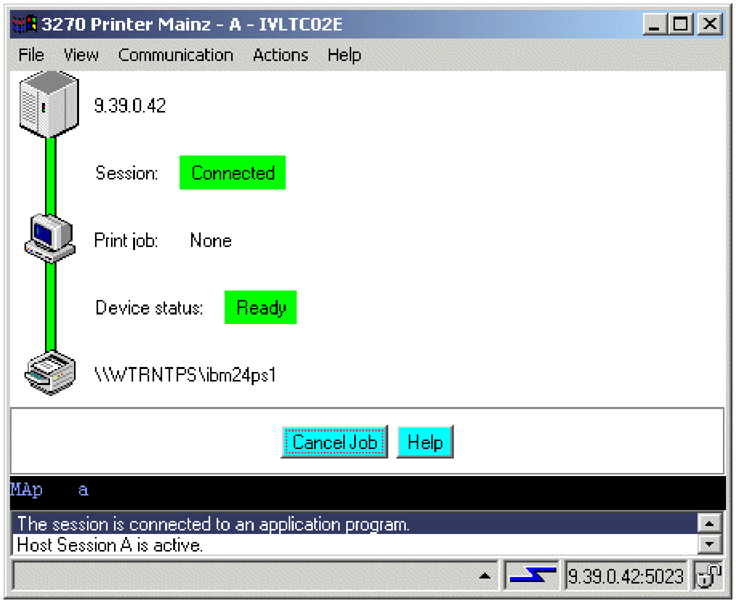
  The default is No (not visible).

- Status Bar

  Determines whether the status bar is visible at the bottom of the window when the session starts (recommended)

21.2.2 Using a 3270 Printer Session

When you start a printer session, you should see a window similar to the one shown in Figure 21-8.



9.39.0.42

Session: Connected

Print job: None

Device status: Ready

\\WTRNTPS\ibm24ps1

The session is connected to an application program.
Host Session A is active.

9.39.0.42:5023

Figure 21-8 Connected 3270 printer session

To send a print job, issue the necessary command in the host application to send print output to the LU as it is named at the host, not as it is named in the communications server.

The session window

This section is a description of what you may do in the session window.

Title Bar

The title of the printer session window includes parameters that you have configured and perhaps an ID that is generated by the system. They appear in the following order, delimited by -:

- The session name (for example, 3270 Printer Mainz)
- The session ID or short name
- The printer LU name (for example, IVLTC02E)

Menu Bar options

The Communication and Help items are much the same as in a display session, but others are different:

- File

This allows you to print a test page, or eject a page. You can also select another printer or modify the page properties without restarting the session. Configurable items that have been locked by the administrator will appear greyed out, and cannot be modified.

Printing a test page causes a page to be printed that contains some standard text that should be formatted correctly. It also serves as a test of the connection between the workstation and the printer; it does not test the link to the server or host.

- View

  From this menu, you can toggle the display of the status bar, the graphic display, and the textual OIA. Switching off the graphic display removes the pictures of the devices and the links between them. Once you are used to the meanings of the status indicators, you may wish to remove the graphics. The textual OIA displays the explanation of the graphical OIA in two lines of text.

Main emulator window

The main emulator window shows the following information:

- IP address or host name of the communications server
- Link status

  The lines between the server, the workstation, and the printer show green or red depending on whether they are connected or not.

- Session status
  - Disconnected

    Indicates that there is no session between Host On-Demand and the Telnet server. If the session is connecting to the host system through a communications server/gateway, this indicates the status of the connection to the server/gateway, not to the host.

  - COMM nnn

    Indicates a communications problem. Note the specific number (nnn), then use the **?** button to get more information. If the status bar is displayed, you can also select the message in the status bar history, and click **?** for help.

  - PROG nnn

    Indicates an error in the print data stream from the host system. Note the specific number (`nnn`), then click the **?** button for more information.

  - Connected

Indicates that Host On-Demand and the Telnet server are connected. If the session is connecting to the host system through a communications server or gateway, this state indicates the status of the connection to the server or gateway, not to the host. However, column 3 of the OIA indicates the status of the host connection, as follows:

An asterisk (*) indicates that the session is connected to an application program (LU-LU connection)

A `p` indicates that the session is connected to a host but not to an application (SSCP-LU connection).

- Print Job

  This field will contain one of the following to describe the status of the print job:

  - None

    Indicates that there are currently no print jobs being sent from the Telnet server.

  - Waiting

    Indicates that Host On-Demand is trying to send a print job to the printer or file. However, it cannot begin or continue the job because of the status of the printer or file.

  - Page `nnn`

    Indicates that page number `nnn` of the print job is currently being printed. This is the page number as viewed by the host; the printer may not be printing that page (3270 only).

  - Canceling

    Indicates that the user has clicked **Cancel Job**. This state will be maintained until the host application has sent the rest of the print job because Cancel Job cannot stop the host application. Host On-Demand must process the rest of the print job, but does not print it. This can take a while for a large print job.

- Device status

  - Ready

    Indicates that the printer or file is active and ready to receive a print job

  - Busy

    Indicates that the printer or file is active but is not available to receive a print job because it is currently being used by another application or session

  - Error

    Indicates that the printer or file cannot be used at this time

  – Printing

    Indicates that the printer or file is currently in use by this session

- Port

  Printer or file to which this session prints

Cancel Job button

There is no architectural way to tell the host application to cancel a print job, so when you click **Cancel Job**, Host On-Demand continues to receive and process each page but does not print it. This may take some time for large print jobs.

PA1 and PA2 buttons

These appear only if they were switched on when the session was configured. There is no point in having them in the window unless one or more of your host applications have been written to respond to them.

Operator information area

Depending on the configuration, the OIA may be visible at the bottom of the window.

As a new feature in Host On-Demand V8 the, OIA can as well be displayed in textural context in two lines, (click at the menu bar **View - Textual OIA**). The last buffered messages can be scrolled. Adjust the session window size horizontally so that the horizontal scroll bar for the text disappears. This is the minimum size for the window so that the maximum of two lines are displayed, and can be read by a screen reader.

Logical configuration

Figure 21-9 shows a 3270 printer session and how it works from a logical (as opposed to the physical) perspective.

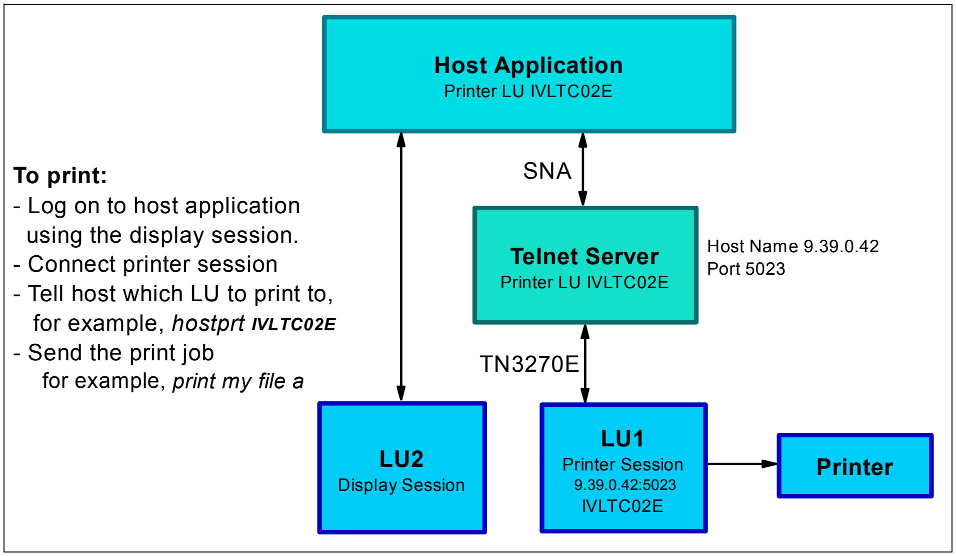

Host Application
Printer LU IVLTC02E
To print:
- Log on to host application using the display session.
- Connect printer session
- Tell host which LU to print to, for example, *hostprt IVLTC02E*
- Send the print job for example, *print my file a*
SNA
Telnet Server
Printer LU IVLTC02E
Host Name 9.39.0.42
Port 5023
TN3270E
LU2
Display Session
LU1
Printer Session
9.39.0.42:5023
IVLTC02E
Printer

Figure 21-9 Logical configuration of 3270 host printing

21.3 3270 Associated Printer Sessions

Telnet servers, such as Communications Server for Windows, or Communications Server for OS/390, can be configured to support the association of a display LU with an associated printer LU. The purpose of this is convenience. You know that when you start the display session, a specific printer session will start; therefore, if you direct your host printing to that session, it will appear on the correct printer. It is also easier to configure an associated printer session, because you do not have to enter the destination address or LU name.

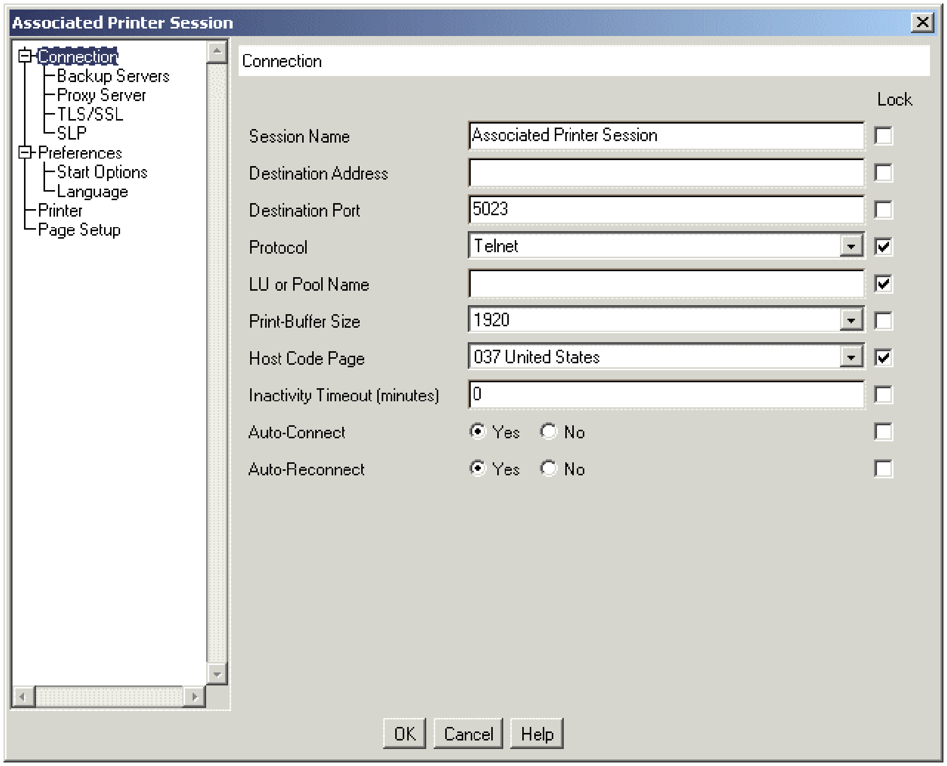
The association between a display and a printer session must be made in the TN3270E communications server. In the Host On-Demand configuration notebook, you can associate the same printer session with more than one display session.

21.3.1 Configuring associated printer sessions

To configure a display session with an associated printer session:

1. Configure a printer session

   Configure the session as usual, but leave the Destination Address blank, as shown in Figure 21-10.

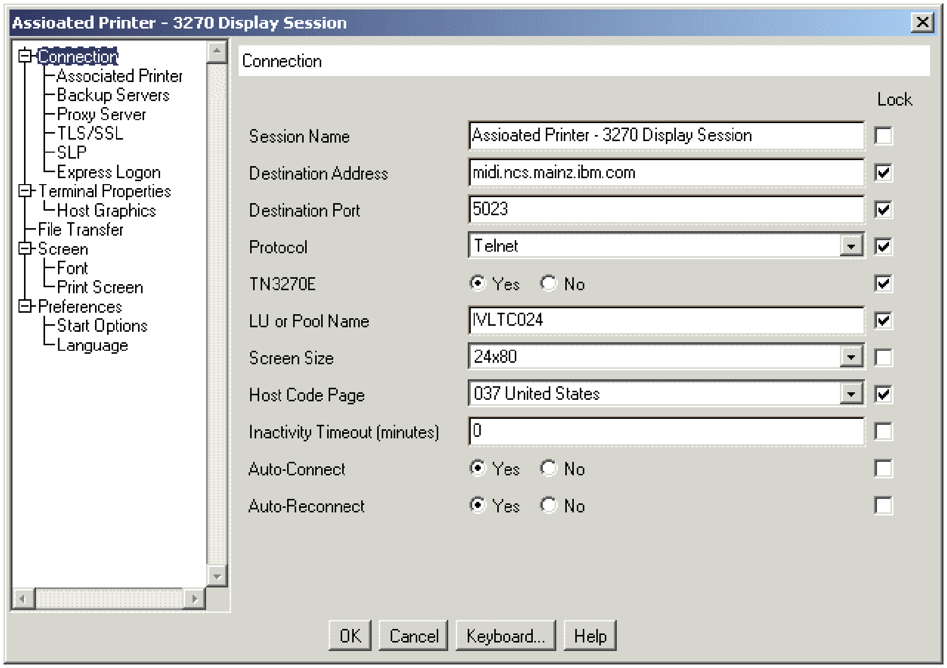


		Lock
Session Name	Associated Printer Session	☐
Destination Address		☐
Destination Port	5023	☐
Protocol	Telnet	☑
LU or Pool Name		☑
Print-Buffer Size	1920	☐
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)	0	☐
Auto-Connect	● Yes ○ No	☐
Auto-Reconnect	● Yes ○ No	☐

Figure 21-10 Configuring an associated printer

2. Create or modify a display session.

   First we start configuring a new display session to the Telnet server as shown in Figure 21-11.



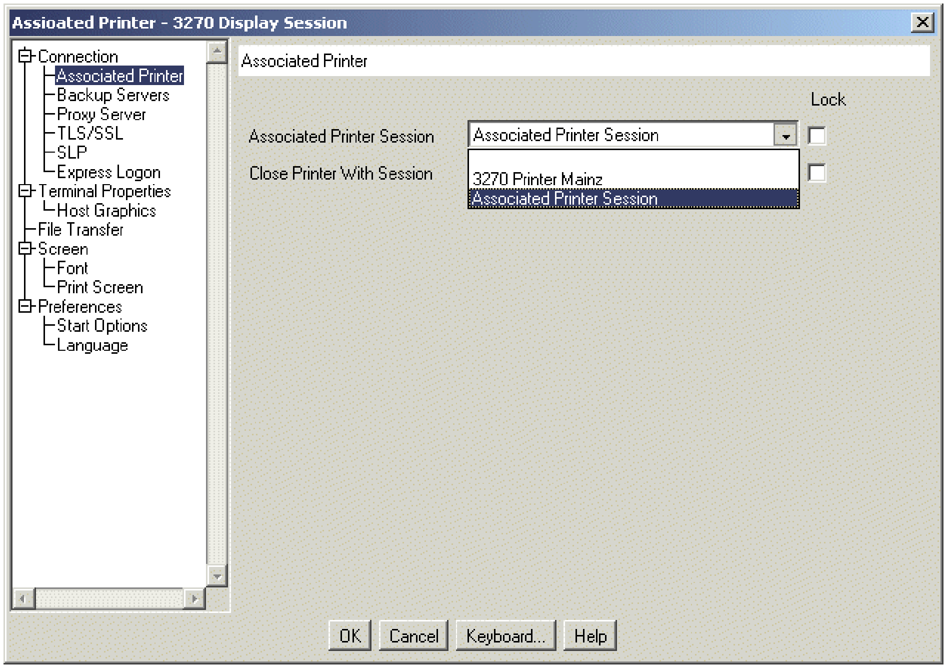
Assioated Printer - 3270 Display Session

Connection

		Lock
Session Name	Assioated Printer - 3270 Display Session	☐
Destination Address	midi.ncs.mainz.ibm.com	☑
Destination Port	5023	☑
Protocol	Telnet	☑
TN3270E	● Yes ○ No	☑
LU or Pool Name	IVLTC024	☑
Screen Size	24x80	☐
Host Code Page	037 United States	☑
Inactivity Timeout (minutes)	0	☐
Auto-Connect	● Yes ○ No	☐
Auto-Reconnect	● Yes ○ No	☐

Figure 21-11 Display session for an associated printer

3. Then select from the tree structure the Associated Printer item. The windows as shown in Figure 21-12 appears. Click the **Associated Printer Session** pull-down box. It lists the available printer sessions. From that list, select the printer session that we configured in Figure 21-10 on page 736.


Assioated Printer - 3270 Display Session

Associated Printer

Associated Printer Session: Associated Printer Session ▾ □ Lock

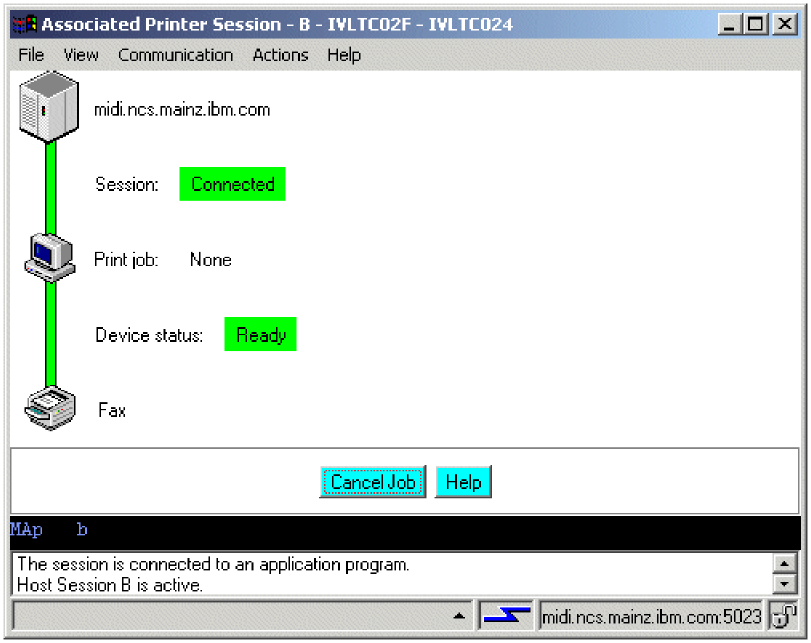
Close Printer With Session □

3270 Printer Mainz
Associated Printer Session

Figure 21-12 Associating a printer session with a 3270 display

4. With the Close Printer With Session parameter, you can force the printer session to be closed when the 3270 session is closed. We recommend this, especially if you are selecting displays and printer sessions from a pool. Doing so ensures that display and printer pairs are always available.

When you start the display session, the associated printer session starts automatically (see Figure 21-13).



midi.ncs.mainz.ibm.com

Session: Connected

Print job: None

Device status: Ready

Fax

MAp b

The session is connected to an application program.
Host Session B is active.

midi.ncs.mainz.ibm.com:5023

Figure 21-13 Associated printer session

The title of the printer session window includes parameters that you have configured and perhaps an ID that is generated by the system. They appear in the following order, delimited by “-”:

- The session name (for example, Associated Printer)
- The session ID or short name
- The printer LU name (for example, IVLTC02F)
- The LU name of the associated display session, if any (for example, IVLTC024)

21.3.2 How an associated printer session works

Figure 21-14 shows an associated printer session, and the logical connections among them.

Display LU IVLTC024 is associated with printer IVLTC02F. Remember that the association itself is made in the Telnet server, not by the host application, or in your emulator configuration. When you configure the display session, you just select (from the Associated Printer Session drop-down list) a printer emulator session that is going to send its output to the correct physical printer. When the display session starts, the Host On-Demand client will automatically issue a request (`Telnet INIT`) for a printer session providing the LU name of the display session. The Communications Server will use the display LU name to locate the associated printer LU name. If a match is found, the LU will be assigned and a session established if the LU is not currently in session. If no match is found, no printer session will be established.

The association does not mean that the host application automatically directs output to the correct LU unless it has been written to do so, because it knows nothing about the association. When you are ready to print, you must tell the host application which printer LU to direct the output. Although you do not necessarily know the name of the printer LU until its session starts, it is available from the printer session's title bar.

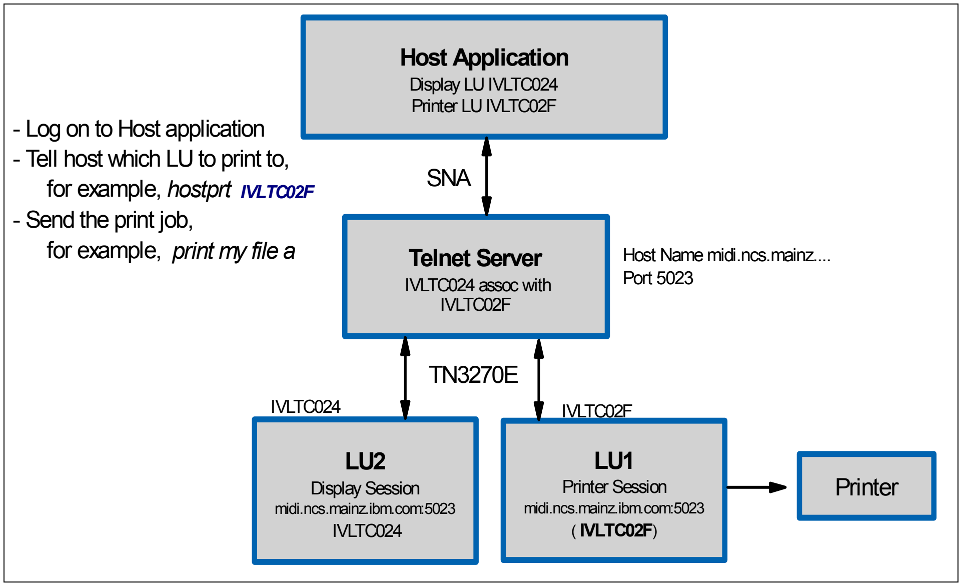


Figure 21-14 How associated display and printer sessions work

21.4 5250 printer session

A Host On-Demand 5250 printer session emulates a 3812 printer attached to an iSeries Server. Host On-Demand 5250 printing is performed using Host Print Transform (HPT).

21.4.1 Host Print Transform

Host Print Transform is an OS/400 function that converts an SNA character string (SCS) or Advanced Function Printer (AFP™) data stream into an ASCII data stream. The ASCII data stream is then formatted and sent to an ASCII printer through a Host On-Demand 5250 printer session. The conversion is done on the iSeries, which provides these advantages:

- Consistent output for most ASCII printers

  HPT is capable of supporting many different types of ASCII data streams. For example, it supports the Hewlett-Packard printer control language (PCL), the IBM personal printer data stream (PPDS), and the Epson FX and LQ data streams.

- 3812 SCS printer emulation

  If HPT is used, all of the ASCII printers connected to an iSeries system can perform a 3812 SCS level of function.

  Your printer may not support all functions. For example, you cannot print in 180-degree orientation if your printer supports only 0 and 90-degree orientations.

- Support for many different ASCII printers

  Many printers, including IBM printers, support HPT.

- Customized printer support

  You can add or change characteristics for a particular printer using workstation-customizing objects that come with HPT. Also, if a workstation-customizing object for a particular printer does not exist, you can create one.

- Support for the conversion of a double-byte SCS or AFP data stream into an ASCII data stream

  For the AFP-to-ASCII data stream conversion, there are additional advantages such as support for AFP font, text, image, and bar code commands. The following types of printers support this function:

  – IBM 4019, 4029, and 4039 laser printers
  – HP laser and ink jet printers
  – IBM PAGES printers (DBCS)

  On other printers, images or bar codes may not be supported by the AFP-to-ASCII transform function, and the text may not be positioned correctly.

How Host Print Transform works

The 5250 Host Print Transform (HPT) converts the iSeries print data stream just before it is sent from the iSeries to the printer spool file. Because the iSeries does the conversion, the host does most of the print processing instead of the workstation.

Many printers, including IBM printers, support the ASCII print-data stream. The ASCII data stream uses iSeries system objects that describe the characteristics of a particular ASCII printer. When you configure a printer session, you select the printer from the list provided.

By default, Host On-Demand uses the SCS-to-ASCII transform, but you can configure the iSeries to do an AFP-to-ASCII transform, which Host On-Demand also supports. The ASCII data stream is passed through the emulator using the SCS ASCII Transparency (`ATRN`) command. Host On-Demand deletes the ASCII Transparency command and passes the ASCII data stream to the workstation printer.

For more information about the Host Print Transform, refer to the iSeries Printer Device Programming documentation.

21.4.2 Configuring a 5250 printer session

There are nine tree and branch items to the 5250 printer definitions:

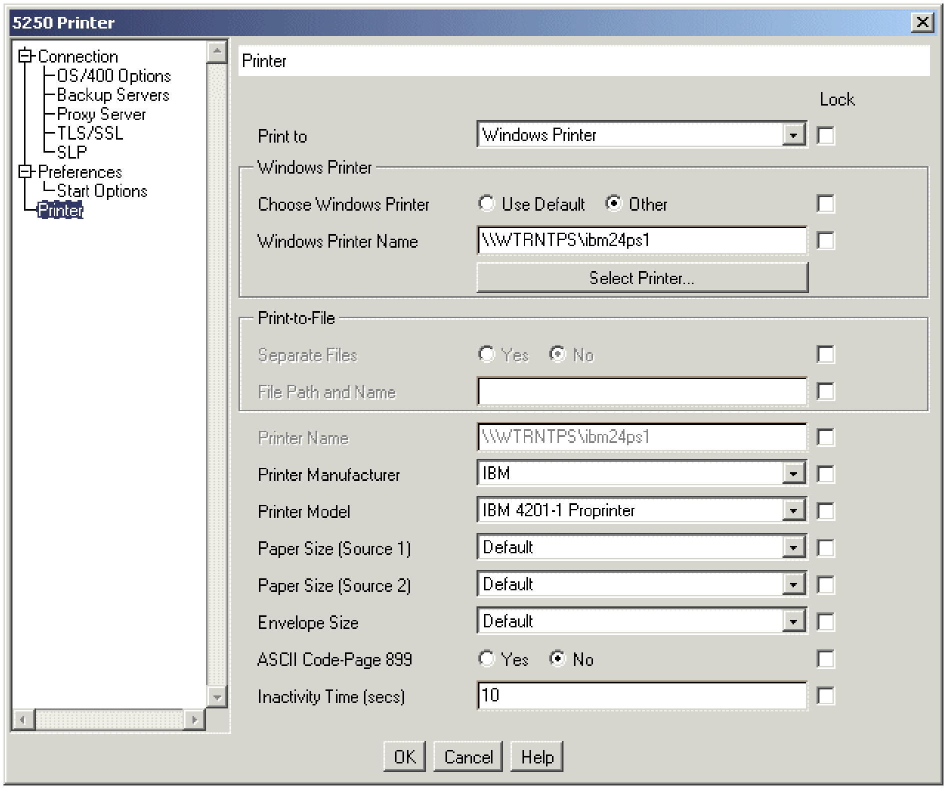
- Connection
  - OS/400 Options
  - Backup Servers
  - Proxy Server
  - TLS/SSL
  - SLP
- Preferences
  - Start Options
- Printer

Except for the Printer item, these are similar to the 5250 display session or are only a subset of the parameters of a display session. Therefore, please refer to “3270 and 5250 Display Sessions” on page 279.

5250 printer Printer item

The Printer item shown in the upper portion of the window shows the generic printer parameters as used for a 3270 printer session. We pointed them out in the 3270 printer session section titled “3270 printer Printer item” on page 722, so please refer to it for this part of the item contents.

The Printer item is also used to define the output device for the print data, and because 5250 printer support uses Host Print Transform (see “How Host Print Transform works” on page 742) we specify characteristics of the target printer.



Printer

		Lock
Print to	Windows Printer	□
Windows Printer		
Choose Windows Printer	○ Use Default ● Other	□
Windows Printer Name	\\WTRNTPS\ibm24ps1	□
Print-to-File		
Separate Files	○ Yes ● No	□
File Path and Name		□
Printer Name	\\WTRNTPS\ibm24ps1	□
Printer Manufacturer	IBM	□
Printer Model	IBM 4201-1 Proprinter	□
Paper Size (Source 1)	Default	□
Paper Size (Source 2)	Default	□
Envelope Size	Default	□
ASCII Code-Page 899	○ Yes ● No	□
Inactivity Time (secs)	10	□

Figure 21-15 Printer item on the 5250 printer session window

- Printer Manufacturer (5250)

  The manufacturer of the printer that will be used for this session.

- Printer Model (5250)

  The model of the printer that will be used for this session.

- Paper Size (source 1) (5250)

  Specifies the size of the paper in Source 1

- Paper Size (source 2) (5250)

  Specifies the size of the paper in Source 2

- Envelope Size (5250)

  Specifies the size of the paper in the envelope feeder

- ASCII Code Page 899 (5250)

  Click **Yes** if your printer supports ASCII code-page 899. This is not resident on most printers.

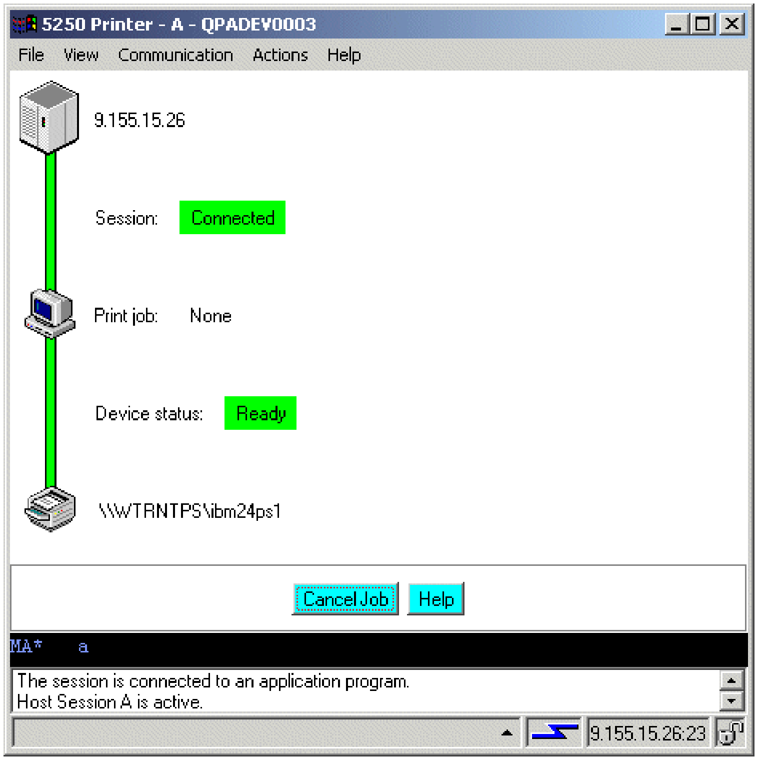
- Inactivity Time (secs) (5250)

  Specifies the amount of time to wait for printing to start. If printing does not start within the time set, an Intervention Required message pops up. The valid values are between 10 and 255 seconds. A value of 0 disables the timer and a message never appears.

  The default is 10.

21.4.3 Using the 5250 printer session

Using the 5250 printer session is very similar to the 3270 printer session discussed in 21.2.2, “Using a 3270 Printer Session” on page 730.



5250 Printer - A - QPADEV0003

9.155.15.26

Session: Connected

Print job: None

Device status: Ready

\\WTRNTPS\ibm24ps1

MA* a

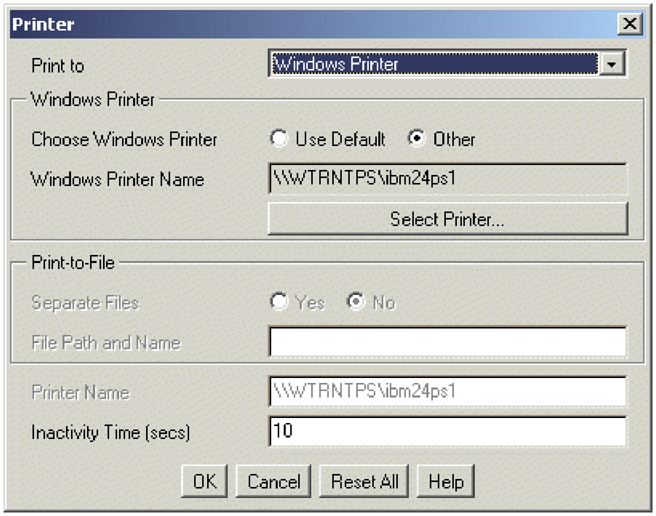
The session is connected to an application program.
Host Session A is active.

9.155.15.26:23

Figure 21-16 5250 printer session

The following exceptions apply:

Selecting **File -> JumpNext** allows the user to jump to the next session. Selecting **File -> Printer** will present the window (shown in Figure 21-17) temporarily modifies printer settings. Printing of a test page, or ejecting a page from the printer is not available for 5250 printer sessions.



Print to: Windows Printer

Windows Printer

Choose Windows Printer ○ Use Default ● Other

Windows Printer Name: \\WTRNTPS\ibm24ps1

Print-to-File

Separate Files ○ Yes ● No

File Path and Name:

Printer Name: \\WTRNTPS\ibm24ps1

Inactivity Time (secs): 10

Figure 21-17 Printer settings available through the menu bar File-Printer

The Print job: field on the main session window will state `Printing` when a print job is currently being printed. This is in contrast to the message `Page nnn`, which is presented for 3270 printer sessions.

21.5 3270 Host printing for DBCS

If you are the user of a Double-Byte Character Set (DBCS) language, it may be necessary to correct some files in order to print and display them with Host On-Demand. DBCS has user-defined characters (UDC), which are unique to the languages supported by Host On-Demand. This section tells you how to print and display DBCS, especially UDC.

Note: Comprehensive documentation and help is available with regard to host printing information. Please refer to the online help.

3270 Host Printing for DBCS is almost the same as for Single-Byte Character Set (SBCS). The following sections provide information about the differences between DBCS and SBCS, and the points that are unique to DBCS.

When you configure a printer session in a DBCS language, you must be careful about the host code page and the printer definition table.

21.5.1 Host code page

Generally, the default host code page, which belongs to the default language of Host On-Demand, has already been selected by the system. In some DBCS languages, there are several code pages in the list, so you should change to the code page supported by the host system if necessary. Use the code page drop down box in the host code page item of your printer session.

21.5.2 Printer definition tables

Host On-Demand and Personal Communications Version 5.7 provide PDTs and PDFs for each language. DBCS printers are different from SBCS, and support the following modes:

- HP PCL Level 3
- IBM PPDS
- ESC/P

The list of available PDTs is determined by the host code page; only PDTs that are valid for the selected code page appear in the pull-down list. You should choose the PDT that is correct for the printer you will use.

The PDT lists for DBCS languages are:

930 Japan (Katakana Extended) and 939 Japan (Latin Extended)

- ASCII text mode
- Printers based on ESC/P 24-J84
- IBM 5577-B02, F02, G02, H02
- IBM 5585-H01 Printer
- IBM 5587 G01, H01 (without advanced function)
- Lips3a4 Printer
- Lips3b4 Printer

933 Korea (Extended)

- Korea IBM 5577 Printer
- Ks_jo Printer
- Ks_wan Printer
- Kssm_jo Printer
- Kssm_wan Printer

935 PRC (Simplified Chinese Extended)

- Simplified Chinese ESC/P Printer

937 ROC (Traditional Chinese Extended)

- Traditional Chinese ESC/P Printer (5550)
- Traditional Chinese ESC/P Printer (Big-5)
- Traditional Chinese ESC/P Printer (cns)
- Traditional Chinese ESC/P Printer (tca)
- Traditional Chinese IBM 5577 Printer
- Traditional Chinese IBM 5585 Printer

If you want to use a PDT other than one in the list, for example a SBCS PDT, you must put the appropriate PDF in the directory \pdfpdt\usrpdf with a different name, then compile it. This creates a unique PDT, which will appear in the PDT pull-down list on the configuration window.

21.5.3 Font image file

When you print user-defined characters (UDC), a UDC font image file is needed; you must create it and copy it to the `\ondemand\Hod\fonts` directory on a server, and to the `\ondemand\lib\fonts` directory on a locally installed client.

For host printing support of user-defined characters (UDCs), in either Java file interface mode or Windows spooler interface mode, you must prepare a UDC font image file. On a server, this file must be located in the \HostOnDemand\hod\fonts\ directory so that it is accessible to clients. In Windows' native printing mode, you do not have to do this as long as UDCs are defined on your Windows system.

UDC support is applicable to double-byte languages only.

On Windows, you must run the **`w32udcnv.exe`** utility to find and convert Windows user-defined fonts into a usable font-image file. The utility is provided in the `\udc` directory on the Host On-Demand CD. It is not copied to the server during installation. To use the utility:

- Run **`w32udcnv.exe`**.
- Click **Convert** to start the conversion and generate a font-image file.

After conversion, the font-image file is saved in the C: drive's root, and is named according to the language of the operating system you are running, as shown in Table 21-1.

Table 21-1 Font-image file names

Platform	Font-image filename
Japanese Windows	jpn24.fnt
Korean Windows	kor24.fnt
Simplified Chinese Windows	chs24.fnt
Traditional Chinese Windows	cht24.fnt

Copy the font image file to the `\HostOnDemand\hod\fonts` directory.

On an OS/2 server, copy the OS/2 font-image file, $SYS1Z24.FNT, to the `\HostOnDemand\hod\fonts` directory and rename it according to Table 21-1.

Limitations

In a Traditional Chinese Windows environment, there are 13 more UDCs than IBM's Big-5 UDCs. Therefore, if the last 13 UDCs are defined in the range of 0xC8F2-0xC8FE, they are ignored by the utility and cannot be used.

In a Korean Windows environment, only PC code page 949 is supported. You can define and print 188 UDCs in the ranges of 0xC9A1-0xC0FE and 0xFEA1-0xFEFE.

21.6 VT host printing

Host On-Demand provides VT host printing in much the same manner as a VT 420 terminal would provide this service to a VT host. You can print host application files on a printer that is directly attached to your workstation or to a network printer.

In a traditional VT host print session, the host determines when a print operation is desired (typically triggered by a user's action). In a VT print session, the same host-terminal connection used for screen-based information is used to pass information to the printer. Once the host determines that a print job is to start, a terminal sequence is sent by the host to the terminal to initiate the desired print operation. The host sends all desired print information and then ends the process by sending a print termination sequence to the terminal. In some cases, both the screen and the printer may be the simultaneous destination of the information sent by the host.

Host On-Demand supports all of the VT 420 defined print sequences; however, due to limitations in the Java environment, not all printer status commands are supported. The Windows spooler interface mode and the Windows native printing modes are not supported on VT host print sessions.

More information on VT Host Printing is contained in the *DEC VT220 Programmer Reference Manual*.

21.7 Adobe PDF printing

The option of Host On-Demand to print 3270 print jobs as Adobe PDF files to disk has the following features and limitations:

- Features:
  - No need to have Adobe Acrobat installed for creating the PDF files
  - Can be browsed and printed with Adobe Acrobat Reader or Acrobat Reader plug-in for browser
  - Unlike a plain text file, Adobe PDF file keeps all formatting information (CPI, LPI, etc.)
- Limitations
  - 3270 Printer Session Only (no 5250, no Print Screen support)
  - Limited font support. For U.S. English, “Courier”, “Courier New” and “Lucid Console” are supported.
  - Fixed top/bottom/left/right margins:
    - 1/4 inch for North American forms (Letter, etc.)
    - 0.5 cm for ISO forms
    - Types of form are also predefined
- NLS considerations
  - Non-Latin 1 SBCS languages (including Bidi, Thai)
    - Embed font file in PDF - Makes file size bigger (100-200K), but runs on all platforms
    - Use Windows font - File size is smaller, but generated file can be browsed only on Windows
  - DBCS languages - Use DBCS fonts provided by Adobe:

    http://www.adobe.com/products/acrobat/acrrasianfontpack.html

    DBCS characters might be browsed without those fonts.

21.8 Host Print JavaBeans

Host On-Demand Version 7 introduced two new beans for host printing:

- HostPrintSession
- HostPrint Terminal

Both beans are available for 3270 and 5250 only. They do not support VT. Both support Java1 (JDK 1.1.8) and Java2 (JDK 1.3.0)

21.8.1 Relationship of Session, HostPrintSession, HostPrintTerminal

- HostPrintSession is an extension of the session bean.
- HostPrintSession is a session.
- HostPrintTerminal is a visual component that contains the HostPrintSession, and thus the session.
- HostPrintTerminal has a HostPrintSession that again is a session.

21.8.2 How to access Host On-Demand beans

There are several JAR files that come with the toolkit. The following JAR files contain all available Host On-Demand beans:

- `habeans.jar` and `habeansnlv.jar` for Java1
- `habeans2.jar` and `habeansnlv2.jar` for Java2

There are two ways to utilize beans within these JAR files:

- Through a visual builder tool that comes with any modern IDE like VisualAge for Java, JBuilder, Visual Cafe, etc.
- By writing the code manually

21.9 ZipPrint

ZipPrint can be used to print any zSeries mainframe file that can be viewed by scrolling through its contents. ZipPrint is designed only for 3270 screens. ZipPrint scrolls through the document or file using the PF-keys assigned for scrolling. While scrolling, ZipPrint takes screen copies of each page and sends the complete set of screen copies to the Windows printer or to a file.

ZipPrint does not have access to a separate LU1 or LU3 print data stream. Like the old-style Print Screen, ZipPrint must extract the data to be printed from the existing LU2 display session.

ZipPrint is implemented as a Host On-Demand macro: When you do a ZipPrint, a macro is generated “on the fly” and is instantly played back. As a macro, ZipPrint can take advantage of the macro runtime's ability to simulate keystrokes, and to read data from the session screen. This ZipPrint macro only exists in memory for the time being executed. *It is not saved*. Only the settings for the printer, page, and profile are saved as parameters within the session properties under the stanza [zipprint].

Before Host On-Demand V8, macros did not have print capability. For ZipPrint, new print action macros have been added, which can be used by user macros as well:

- Initialize printer:

  ```
  <print action="start" windowsPrinterName="Generic / Text Only"
  assigntovar="" />
  ```

- Send data to printer:

  ```
  <print action="extract" srow="1" scol="1" erow="-1" ecol="-1"
  assigntovar="" />
  ```

- Close printer, end the print job:

  ```
  <print action="end" assigntovar="" />
  ```

Here are the steps that ZipPrint follows when it prints a document. As an example, suppose that you are viewing page 4 of a 10-page document and that you click **File -> ZipPrint -> Print From Application - Auto**:

1. ZipPrint scans the screen and chooses the profile by comparing the keyword of the displayed screen with the keyword configured in the available profiles.
2. ZipPrint simulates the page-back key until it reaches page 1 of the document.
3. ZipPrint reads the text from each page and sends the text to the print destination, simulating the page-forward key after each page to advance to the next page.
4. ZipPrint stops when it has processed the last page of the document.
5. Optionally, you can configure ZipPrint to position the document back at the original page after it has processed all the pages for printing. In this example, ZipPrint would position the document back to page 4.

You can see ZipPrint processing the pages when you print a document. You see ZipPrint paging back to the first page, then paging forward to the last page, and (if this option is set) finally paging back to the page that was displayed when the ZipPrint was initiated.

ZipPrint can process up to 10,000 pages in one printing.

21.9.1 ZipPrint configuration steps

ZipPrint is configured in three steps:

1. Setting up the printer or output file
2. Setting up the appearance on the print pages
3. Configuring ZipPrint for screen recognition and scrolling

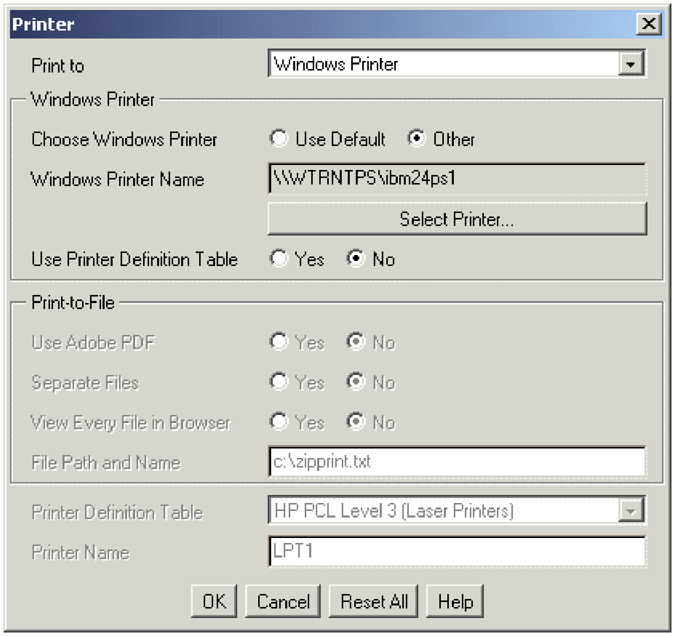
> **Note:** Additional explanation for configuring ZipPrint is located in the ZipPrint Tutorial, and as well in the Host On-Demand InfoCenter.

21.9.2 Configuring ZipPrint to print with the VM text editor XEDIT

In the following example, ZipPrint is configured so that it prints a VM text file edited with XEDIT.

Printer Setup

From the Menu Bar of a display session click **File -> ZipPrint -> Printer Setup.** From the drop down box Print to select the **Windows Printer**. The Printer setup windows as shown in Figure 21-18 is displayed.



Printer

Print to: Windows Printer

Windows Printer

Choose Windows Printer: ○ Use Default ● Other

Windows Printer Name: \\WTRNTPS\ibm24ps1

Select Printer...

Use Printer Definition Table: ○ Yes ● No

Print-to-File

Use Adobe PDF: ○ Yes ● No

Separate Files: ○ Yes ● No

View Every File in Browser: ○ Yes ● No

File Path and Name: c:\zipprint.txt

Printer Definition Table: HP PCL Level 3 (Laser Printers)

Printer Name: LPT1

Figure 21-18 ZipPrint Printer Setup

Select the **Other** radio button from the Choose Windows Printer options.

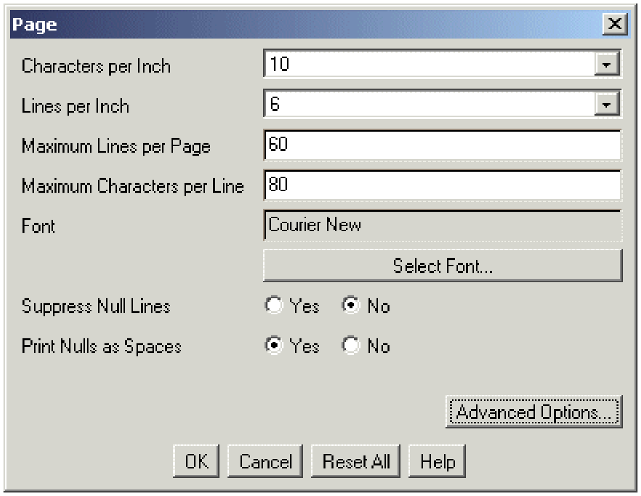
Click the **Select Printer** button and select the printer of your choice.

We do not use the printer definition table.

The other available options are greyed out and are not available because we do not print to a file and are not using a PDF.

Page Setup

From the Menu Bar of the display session click **File -> ZipPrint -> Page Setup**. The window as shown in Figure 21-19 appears.

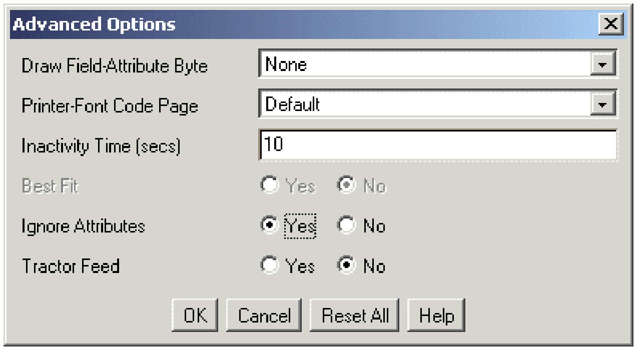


Characters per Inch: 10
Lines per Inch: 6
Maximum Lines per Page: 60
Maximum Characters per Line: 80
Font: Courier New
Suppress Null Lines: ○ Yes ● No
Print Nulls as Spaces: ● Yes ○ No

Figure 21-19 ZipPrint Page Setup

The default values have been used. For printing mainframe documents, it is suggested to keep a non-proportional font as the default courier because mainframe green screen contents are always non-proportional too.

We selected in the **Advanced Options** panel (Figure 21-20) the radio button **Ignore Attributes = Yes**. With the default = No, the printout shows for each screen page one bold line. (In the XEDIT screen the current line is displayed as highlighted.)



Draw Field-Attribute Byte: None

Printer-Font Code Page: Default

Inactivity Time (secs): 10

Best Fit ○ Yes ● No

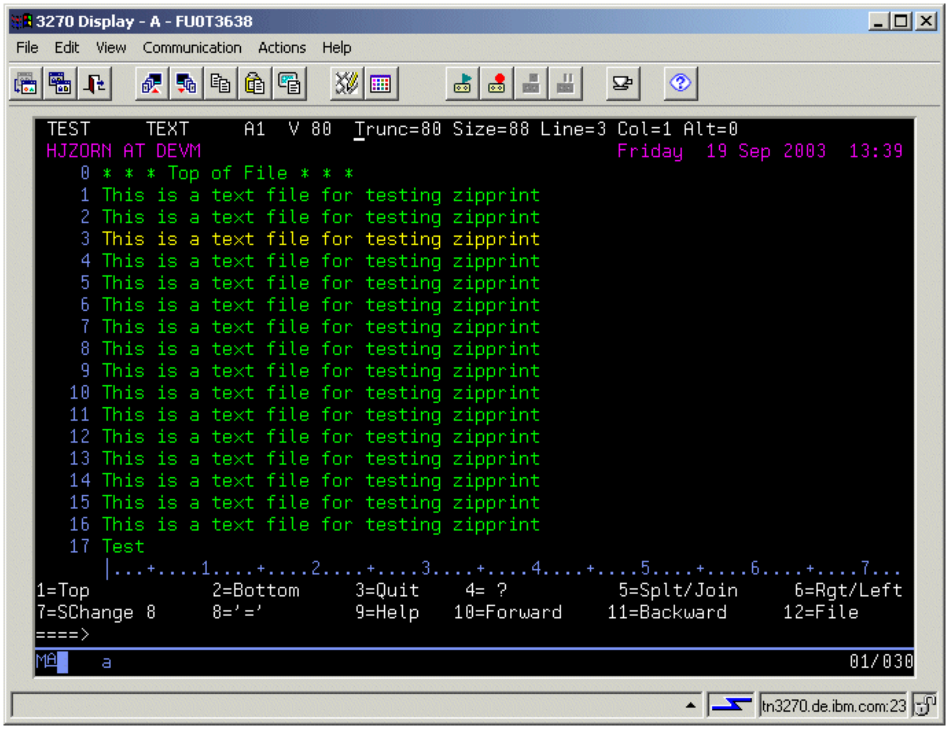
Ignore Attributes ● Yes ○ No

Tractor Feed ○ Yes ● No

Figure 21-20 Advanced Options of ZipPrint Page Setup

Configuring ZipPrint

Log on to VM and display a text file with the application that will be used with ZipPrint. Examine each screen and find a a string which is unique to the application (=XEDIT) so that ZipPrint can distinguish it from other applications that will be used with ZipPrint. This will allow ZipPrint to select the correct profile when you use **Print from Application - Auto.** Move the cursor to the first character of that unique string and note the cursor position, which is displayed in the lower right corner of the OIA. See Figure 21-21 for an example.

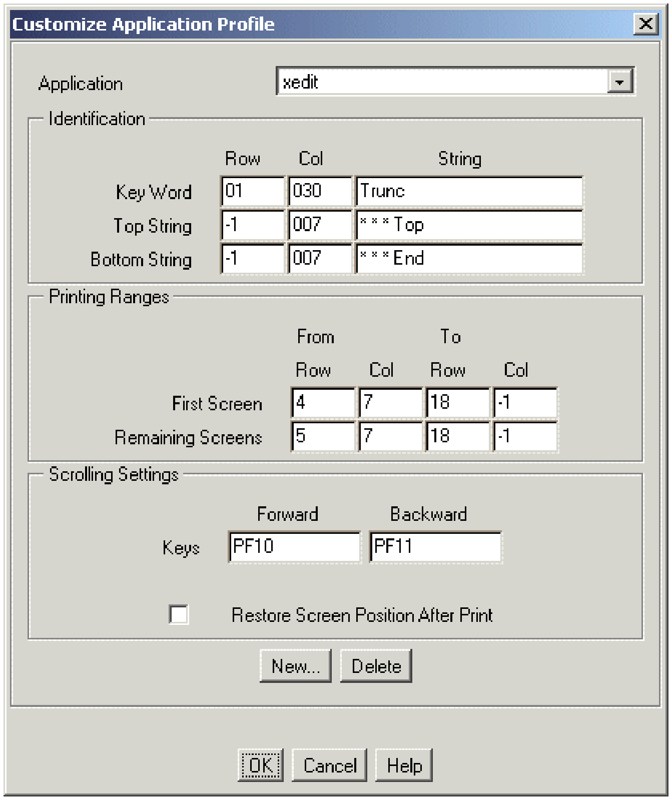

3270 Display - A - FU0T3638
File Edit View Communication Actions Help
tn3270.de.ibm.com:23

```
 TEST     TEXT     A1  V 80  Trunc=80 Size=88 Line=3 Col=1 Alt=0
 HJZORN AT DEVM                                      Friday  19 Sep 2003  13:39
    0 * * * Top of File * * *
    1 This is a text file for testing zipprint
    2 This is a text file for testing zipprint
    3 This is a text file for testing zipprint
    4 This is a text file for testing zipprint
    5 This is a text file for testing zipprint
    6 This is a text file for testing zipprint
    7 This is a text file for testing zipprint
    8 This is a text file for testing zipprint
    9 This is a text file for testing zipprint
   10 This is a text file for testing zipprint
   11 This is a text file for testing zipprint
   12 This is a text file for testing zipprint
   13 This is a text file for testing zipprint
   14 This is a text file for testing zipprint
   15 This is a text file for testing zipprint
   16 This is a text file for testing zipprint
   17 Test
      |...+....1....+....2....+....3....+....4....+....5....+....6....+....7...
1=Top           2=Bottom     3=Quit    4= ?          5=Splt/Join      6=Rgt/Left
7=SChange 8     8='='        9=Help    10=Forward    11=Backward     12=File
====>
MA      a                                                                01/030
```

Figure 21-21 VM screen showing text using XEDIT

> **Important:** Remember that ZipPrint may be invoked from any screen of the application. So the unique string has to be on every screen.

From the menu bar click **File -> ZipPrint -> Customize Profiles**. Then click **New** and enter a name for the new profile. The panel shown in Figure 21-22 is displayed.



Application: xedit

Identification

	Row	Col	String
Key Word	01	030	Trunc
Top String	-1	007	* * * Top
Bottom String	-1	007	* * * End

Printing Ranges

	From		To	
	Row	Col	Row	Col
First Screen	4	7	18	-1
Remaining Screens	5	7	18	-1

Scrolling Settings

	Forward	Backward
Keys	PF10	PF11

□ Restore Screen Position After Print

Figure 21-22 ZipPrint - configuring screen identification and scroll keys

Fill in the fields as described in the following examples:

- Key Word: A string which appears on every screen of the document and which is unique for this application. Also enter its row and column. At start ZipPrint will scan the screen searching for that string before it will start to find the top of file and before printing.
- Top String: A string which is unique for the screen when displaying the top of document. It is entered along with its starting column and row. Using XEDIT this string might appear in a different row, depending on how you manoeuvred within XEDIT. Therefore, we use in our example -1 as row number. This is the value for any row. ZipPrint will use this information while scrolling backwards until it finds this string as the top of document before it starts to print. If this screen cannot be found by ZipPrint, ZipPrint loops scrolling until a time out occurs and an error message will be posted. In that case, wait for this time out, clear the error message, and correct the error.

- Bottom String: Same as for Top String. This screen information is used by ZipPrint to recognize the end of the print data. When this screen is encountered, ZipPrint processes this screen and ends.
- Printing Rages: Using this pane, we can choose what part of the screens are printed. On a continuos printout of many pages, we do not want to see the file information, PF key assignment, and so on for each screen. In addition, for some applications, scrolling repeats the last row of the previous screen as the top row of the next screen (that row is displayed on both screens - it overlaps). In addition, many applications show different header and footer information in the first screen than for the following screens. ZipPrint can be configured for the first screen and follow up screens separately. The *from* values for rows and columns have to be entered exactly. For the *to* values for column and row, the entry -1 can be used to indicated that all characters to the end of line or all rows have to be printed. Setting up those values might require some trial and error. We tested it using VM XEDIT and BROWSE.
- Scrolling Settings: Enter the PF key value that will be used for scrolling the screens.
- Restore Screen Position After Print: This field is not checked by default because after printing the application will be ended, and there is no need to wait until ZipPrint has scrolled back to top. If this field is marked, ZipPrint will scroll back to the initial screen (which is the screen from which ZipPrint was invoked = *not always the top of file*).

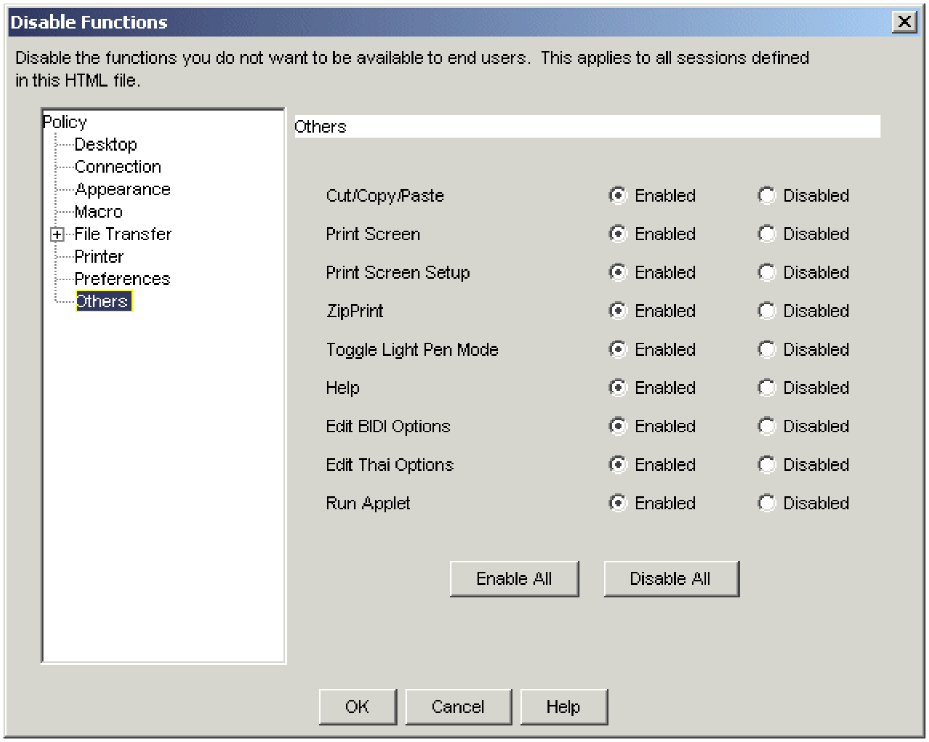
Note: ZipPrint will store the complete initial screen and tries to match that when returning. It will not find the initial screen again, for example if:

- The initial screen contained a time stamp with seconds which changed.
- Scrolling does not return to the exact initial line positioning (e.g. in XEDIT).
- Messages are displayed only once on the first screen when the application is started.

Using this setup, we get the complete text printed without the prefix area, and without the header information and PF-key settings appearing on the screen. However, the printout shows on each.

21.9.3 How to enable ZipPrint

ZipPrint is enabled by default. When using the Deployment Wizard, the administrator can disable the ZipPrint function in the Disable Function panel as shown in Figure 21-23.



Disable Functions

Disable the functions you do not want to be available to end users. This applies to all sessions defined in this HTML file.

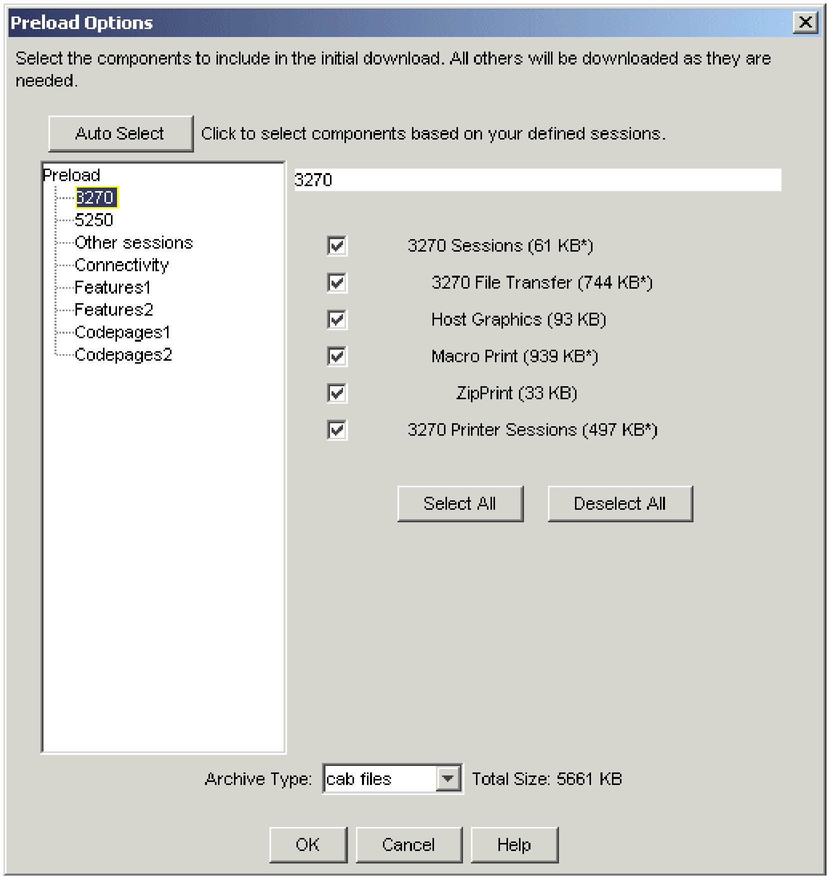
Others

Cut/Copy/Paste	● Enabled	○ Disabled
Print Screen	● Enabled	○ Disabled
Print Screen Setup	● Enabled	○ Disabled
ZipPrint	● Enabled	○ Disabled
Toggle Light Pen Mode	● Enabled	○ Disabled
Help	● Enabled	○ Disabled
Edit BIDI Options	● Enabled	○ Disabled
Edit Thai Options	● Enabled	○ Disabled
Run Applet	● Enabled	○ Disabled

Figure 21-23   Disable Function for ZipPrint in Deployment Wizard

21.9.4 How to preload ZipPrint

In Deployment Wizard window Additional Options click the button **Preload Options**. The panel for selecting Preload Options as show in Figure 21-24 appears. For 3270 sessions the administrator can disable the initial download of the ZipPrint function.



Preload Options

Select the components to include in the initial download. All others will be downloaded as they are needed.

Click to select components based on your defined sessions.

3270

☑ 3270 Sessions (61 KB*)

☑ 3270 File Transfer (744 KB*)

☑ Host Graphics (93 KB)

☑ Macro Print (939 KB*)

☑ ZipPrint (33 KB)

☑ 3270 Printer Sessions (497 KB*)

Archive Type: cab files

Total Size: 5661 KB

Figure 21-24 Preload Option for ZipPrint

21.9.5 Problem Determination

Tracing ZipPrint

Use a client with problem determination enabled. From the display session's menu bar click **Actions -> Problem Determination -> Trace Facility.** The panel shown in Figure 21-25 appears. Select **Function Host On-Demand, Component ZipPrint, Trace Level 3** and select the radio button **Start**. Now run the ZipPrint. After it has finished, select radio button **Stop** and click the **Save** button.

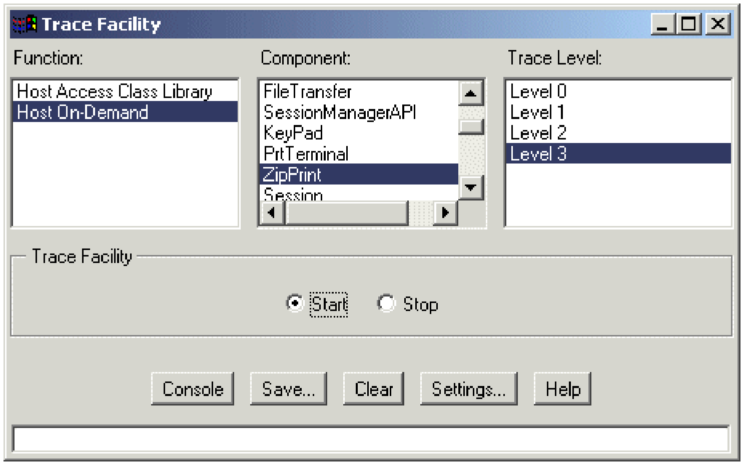
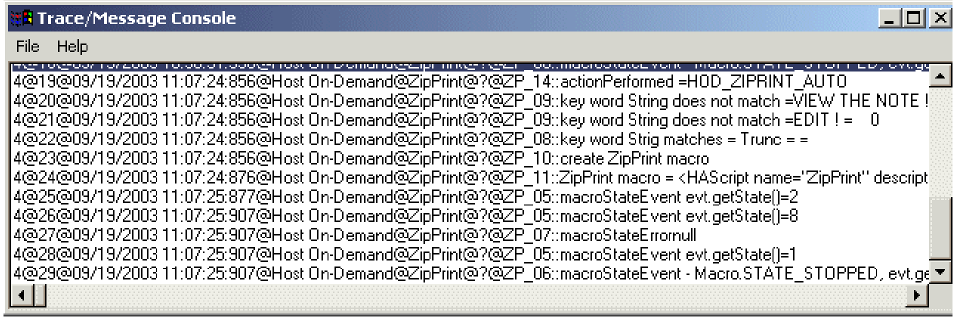


Figure 21-25 Tracing ZipPrint

After the trace has been taken, the macro which has been dynamically created by ZipPrint can be seen in the console. See Figure 21-26.



```
4@19@09/19/2003 11:07:24:856@Host On-Demand@ZipPrint@?@ZP_14::actionPerformed =HOD_ZIPRINT_AUTO
4@20@09/19/2003 11:07:24:856@Host On-Demand@ZipPrint@?@ZP_09::key word String does not match =VIEW THE NOTE !
4@21@09/19/2003 11:07:24:856@Host On-Demand@ZipPrint@?@ZP_09::key word String does not match =EDIT ! =    0
4@22@09/19/2003 11:07:24:856@Host On-Demand@ZipPrint@?@ZP_08::key word Strig matches = Trunc = =
4@23@09/19/2003 11:07:24:856@Host On-Demand@ZipPrint@?@ZP_10::create ZipPrint macro
4@24@09/19/2003 11:07:24:876@Host On-Demand@ZipPrint@?@ZP_11::ZipPrint macro = <HAScript name='ZipPrint'' descript
4@25@09/19/2003 11:07:25:877@Host On-Demand@ZipPrint@?@ZP_05::macroStateEvent evt.getState()=2
4@26@09/19/2003 11:07:25:907@Host On-Demand@ZipPrint@?@ZP_05::macroStateEvent evt.getState()=8
4@27@09/19/2003 11:07:25:907@Host On-Demand@ZipPrint@?@ZP_07::macroStateErrornull
4@28@09/19/2003 11:07:25:907@Host On-Demand@ZipPrint@?@ZP_05::macroStateEvent evt.getState()=1
4@29@09/19/2003 11:07:25:907@Host On-Demand@ZipPrint@?@ZP_06::macroStateEvent - Macro.STATE_STOPPED, evt.ge
```

Figure 21-26 Console with trace of ZipPrint

Look for a line containing `<HAScript name="ZipPrint"`. For example:

```
4@13@09/19/2003 10:58:44:107@Host On-Demand@ZipPrint@?@ZP_11::ZipPrint
macro = <HAScript name="ZipPrint" description="
```

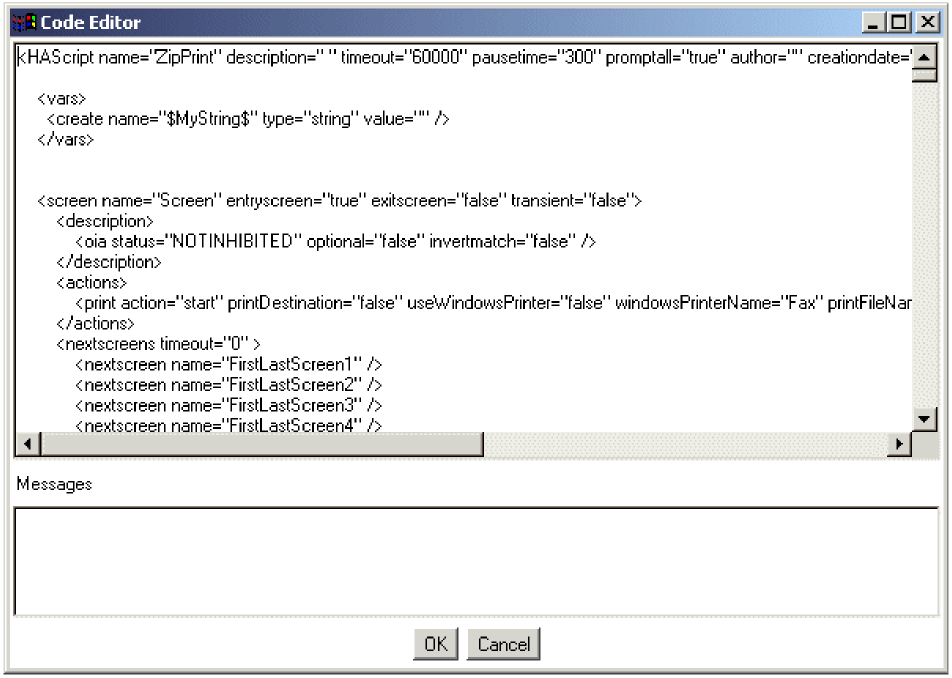
Using CTL-C, this line can be copied to the clip board between the beginning:

```
<HAScript name="ZipPrint"
```

and the ending:

```
</HAScript>
```

Using the *Macro Manager Code Editor* this string can be pasted into the Macro Editor window. The complete macro will still be seen as a single line. Save this Macro and re-open it with the Code Editor. Now the macro can be seen as a normal multi line macro and can be debugged as such (Figure 21-27).



```
<HAScript name="ZipPrint" description=" " timeout="60000" pausetime="300" promptall="true" author="" creationdate='

  <vars>
    <create name="$MyString$" type="string" value="" />
  </vars>


  <screen name="Screen" entryscreen="true" exitscreen="false" transient="false">
    <description>
      <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
    </description>
    <actions>
      <print action="start" printDestination="false" useWindowsPrinter="false" windowsPrinterName="Fax" printFileNar
    </actions>
    <nextscreens timeout="0" >
      <nextscreen name="FirstLastScreen1" />
      <nextscreen name="FirstLastScreen2" />
      <nextscreen name="FirstLastScreen3" />
      <nextscreen name="FirstLastScreen4" />
```

Figure 21-27 Macro code editor with ZipPrint macro

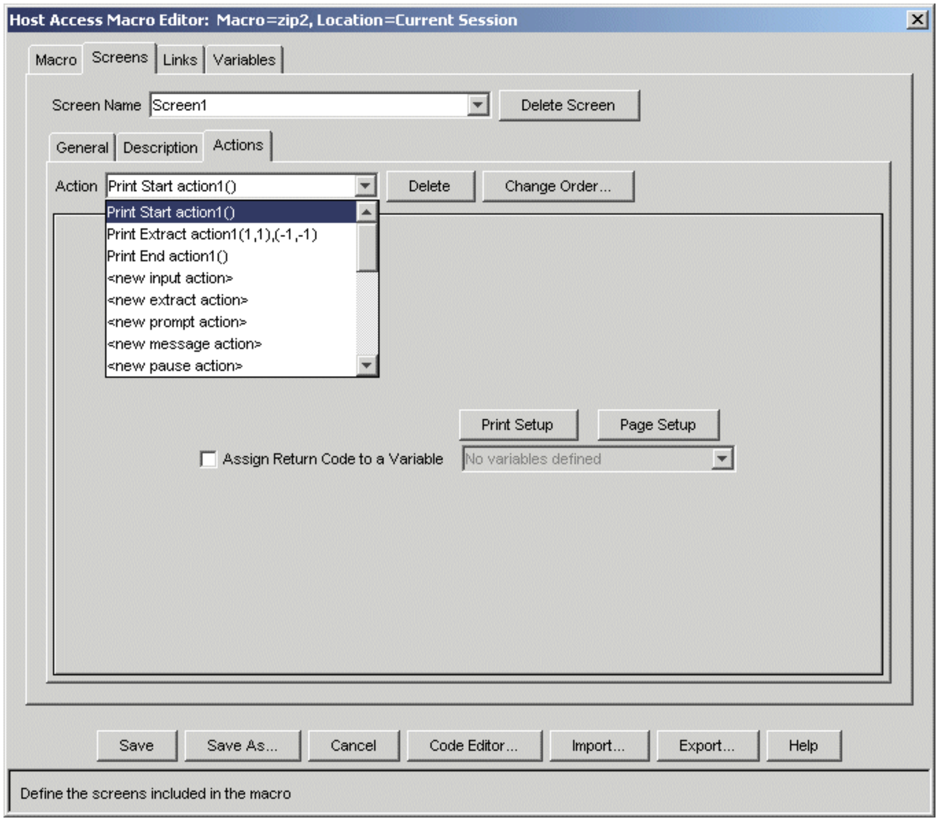
21.9.6 Using new printer macros in customer written macros

The three new printer macros which have been introduced by ZipPrint can be accessed in the macro editor:

- Print Start Action()
- Print Extract Action()

- Print End Action()

Click the **Actions** pull down menu as shown in Figure 21-28. Use as well as the **Print Setup** and **Page Setup** in that window for defining the print destination and its form.



Host Access Macro Editor: Macro=zip2, Location=Current Session

Screen Name: Screen1

Action: Print Start action1()

Print Start action1()
Print Extract action1(1,1),(-1,-1)
Print End action1()
<new input action>
<new extract action>
<new prompt action>
<new message action>
<new pause action>

☐ Assign Return Code to a Variable: No variables defined

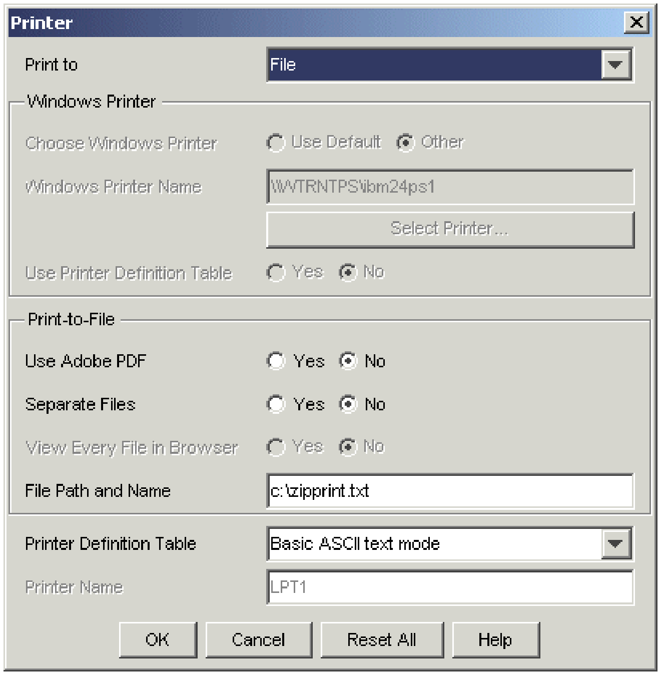
Define the screens included in the macro

Figure 21-28 Using new print macros

As an example we wrote a macro with the Host On-Demand Macro Editor using those three new functions.The macro will take a screen copy and will send it to the printer.

To configure the printer and page setup, click the buttons **Print Setup** and **Page Setup** as shown on Figure 21-28.

In our example we are printing to a file as shown in Figure 21-29.



Print to: File

Windows Printer

Choose Windows Printer ○ Use Default ● Other

Windows Printer Name \\WTRNTPS\ibm24ps1

Use Printer Definition Table ○ Yes ● No

Print-to-File

Use Adobe PDF ○ Yes ● No

Separate Files ○ Yes ● No

View Every File in Browser ○ Yes ● No

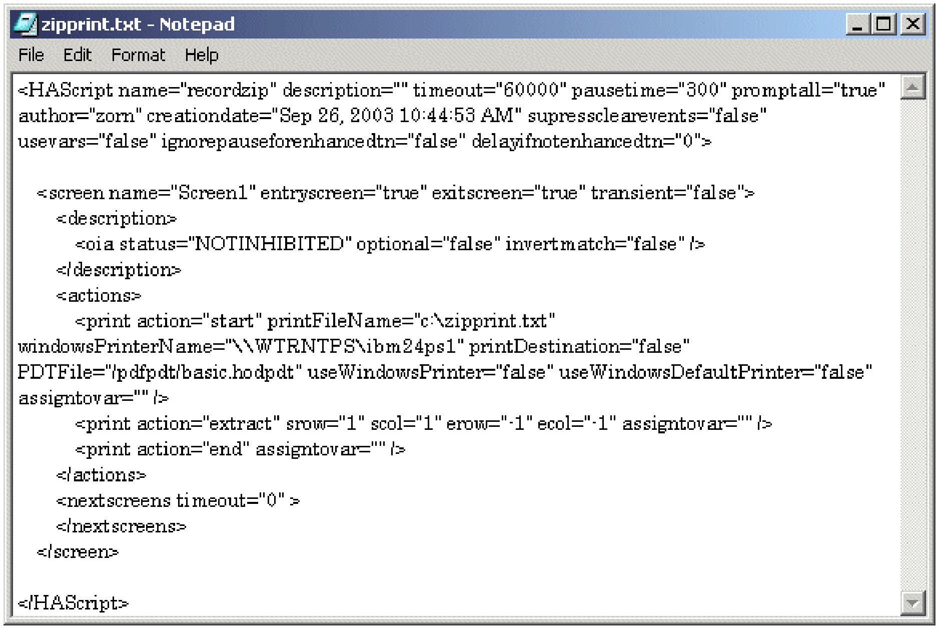
File Path and Name c:\zipprint.txt

Printer Definition Table Basic ASCII text mode

Printer Name LPT1

Figure 21-29 Select print output for printer functions in macro editor

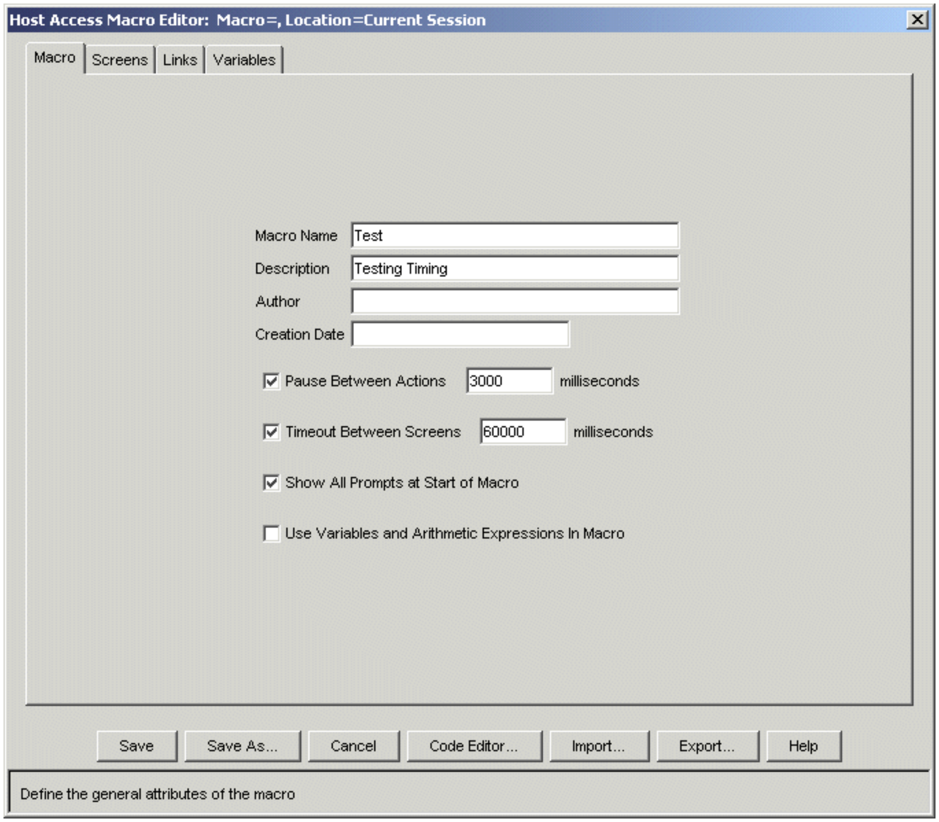
For the macro, see the example of Figure 21-30. You must use the new functions in the correct sequence as shown. Note that two of the command lines are wrapped in the example window.



```
<HAScript name="recordzip" description="" timeout="60000" pausetime="300" promptall="true"
author="zorn" creationdate="Sep 26, 2003 10:44:53 AM" supressclearevents="false"
usevars="false" ignorepauseforenhancedtn="false" delayifnotenhancedtn="0">

  <screen name="Screen1" entryscreen="true" exitscreen="true" transient="false">
    <description>
      <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
    </description>
    <actions>
      <print action="start" printFileName="c:\zipprint.txt"
windowsPrinterName="\\WTRNTPS\ibm24ps1" printDestination="false"
PDTFile="/pdfpdt/basic.hodpdt" useWindowsPrinter="false" useWindowsDefaultPrinter="false"
assigntovar="" />
      <print action="extract" srow="1" scol="1" erow="-1" ecol="-1" assigntovar="" />
      <print action="end" assigntovar="" />
    </actions>
    <nextscreens timeout="0" >
    </nextscreens>
  </screen>

</HAScript>
```

Figure 21-30 Macro written with macro code editor using new print macros

Depending on some environmental impacts, your macro might not run as expected. For example, we have seen in rare cases where ZipPrint itself, as well if ZipPrint traced and was played back as a macro, scrolling could be impacted. In such cases, you can change the default value of the parameter `pausetime=`”300” to a longer wait time. You see this parameter in the first line of the macro in Figure 21-30, and as well in the macro editor window as shown in Figure 21-31. In that window, it is referred to as `Pause Between Actions`. In that example we changed the value from the default 300 to 3000 milliseconds. So, all tasks have more time to settle before the following actions will continue. With this change, the scrolling problem which we observed once during tests was solved.



Macro Name: Test
Description: Testing Timing
Author:
Creation Date:
☑ Pause Between Actions 3000 milliseconds
☑ Timeout Between Screens 60000 milliseconds
☑ Show All Prompts at Start of Macro
☐ Use Variables and Arithmetic Expressions In Macro

Define the general attributes of the macro

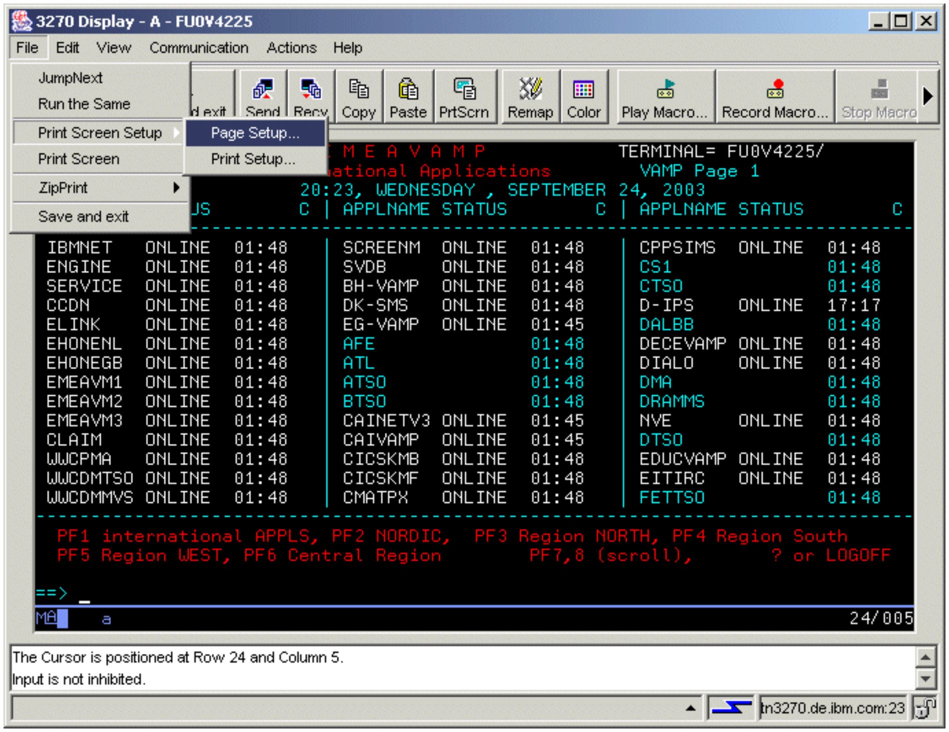
Figure 21-31 Pausetime parameter in Macro Editor window

21.10 Screen copy

The screen copy functions allow one to quickly print the contents of a 3270, 5250, and VT display session to a printer.

21.10.1 Using screen copy

First you can configure the Page Setup and Printer Setup by clicking from the menu bar **File -> Print Screen Setup** as shown in Figure 21-32. This item will *not* be displayed on JAVA 1 clients.

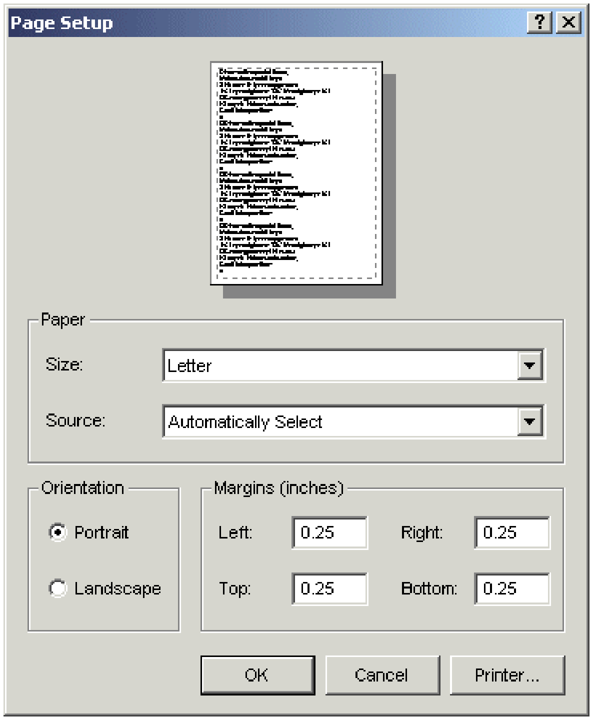


```
                            M E A V A M P           TERMINAL= FU0V4225/
                           ational Applications       VAMP Page 1
                        20:23, WEDNESDAY , SEPTEMBER 24, 2003
                 US          C | APPLNAME STATUS          C | APPLNAME STATUS          C
 ------------------------------------------------------------------------------------
  IBMNET    ONLINE   01:48    | SCREENM  ONLINE   01:48   | CPPSIMS  ONLINE   01:48
  ENGINE    ONLINE   01:48    | SVDB     ONLINE   01:48   | CS1               01:48
  SERVICE   ONLINE   01:48    | BH-VAMP  ONLINE   01:48   | CTSO              01:48
  CCDN      ONLINE   01:48    | DK-SMS   ONLINE   01:48   | D-IPS    ONLINE   17:17
  ELINK     ONLINE   01:48    | EG-VAMP  ONLINE   01:45   | DALBB             01:48
  EHONENL   ONLINE   01:48    | AFE               01:48   | DECEVAMP ONLINE   01:48
  EHONEGB   ONLINE   01:48    | ATL               01:48   | DIALO    ONLINE   01:48
  EMEAVM1   ONLINE   01:48    | ATSO              01:48   | DMA               01:48
  EMEAVM2   ONLINE   01:48    | BTSO              01:48   | DRAMMS            01:48
  EMEAVM3   ONLINE   01:48    | CAINETV3 ONLINE   01:45   | NVE      ONLINE   01:48
  CLAIM     ONLINE   01:48    | CAIVAMP  ONLINE   01:45   | DTSO              01:48
  WWCPMA    ONLINE   01:48    | CICSKMB  ONLINE   01:48   | EDUCVAMP ONLINE   01:48
  WWCDMTSO  ONLINE   01:48    | CICSKMF  ONLINE   01:48   | EITIRC   ONLINE   01:48
  WWCDMMVS  ONLINE   01:48    | CMATPX   ONLINE   01:48   | FETTSO            01:48
 ------------------------------------------------------------------------------------
   PF1 international APPLS, PF2 NORDIC,  PF3 Region NORTH, PF4 Region South
   PF5 Region WEST, PF6 Central Region        PF7,8 (scroll),       ? or LOGOFF

==> _
MA     a                                                                  24/005
```

The Cursor is positioned at Row 24 and Column 5.
Input is not inhibited.

Figure 21-32 Print Screen Setup

Page Setup



Size: Letter

Source: Automatically Select

● Portrait

○ Landscape

Margins (inches)

Left: 0.25

Right: 0.25

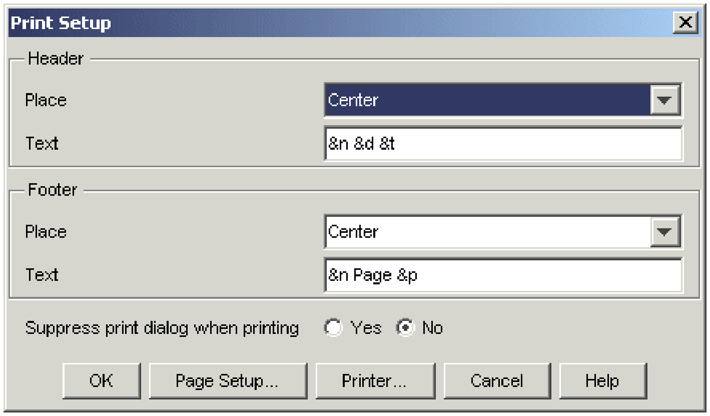
Top: 0.25

Bottom: 0.25

Figure 21-33 Screen Copy Page Setup

The fields are similar to the setup for Wordpad.

Print Setup



Print Setup

Header

Place: Center

Text: &n &d &t

Footer

Place: Center

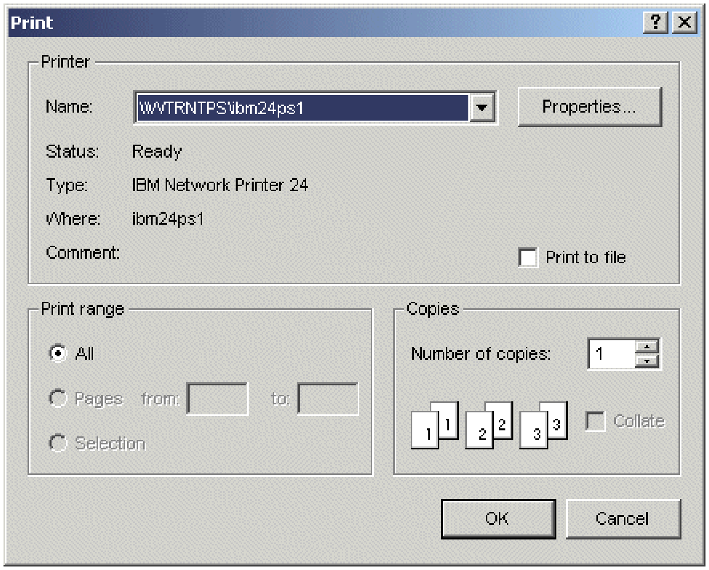
Text: &n Page &p

Suppress print dialog when printing ○ Yes ● No

Figure 21-34 Screen Copy Print Setup

For a detailed description of the fields and possible special strings for the header and footer, click the **Help** key on this window. In our example, we used `&n` for adding a new line for more spacing to the header and footer lines. We printed (centered in the header line) the date and time, and centered in the footer line the word page and the page number. Host On-Demand will scale the printout out of text or graphics so that it fills the page from margin to margin (either from top to bottom, or from left to right depending on the orientation and the screen format). The headers and footers will be added to the top and bottom of the paper. The page number will always be `1` on screen copies - even if the number of screen copies is more than 1 in the Print setup window.

Finally, to initiate the screen copy, select from the menu bar **File -> Print Screen** (or use the **PrtScrn Icon** from the icon bar). The Print window of your operating system comes up. The Windows version is shown in Figure 21-35.



Printer

Name: \\WTRNTPS\ibm24ps1

Status: Ready

Type: IBM Network Printer 24

Where: ibm24ps1

Comment:

□ Print to file

Print range

● All

○ Pages from: to:

○ Selection

Copies

Number of copies: 1

□ Collate

Figure 21-35 Print window of operating system

The screen copy for text ignores all screen attributes and the printout will be in plain black and white (no grey scales on non-color printers). However, the screen copies of host graphics are grey scaled on black and white printers.

Note: The settings for the printer and page setup are independent for screen copy, ZipPrint, and also from those defined within macros.

21.11 Changing and using PDF files

This section is an overview with an example of how to make use of printer definition files (PDF). More details are in the Host On-Demand *Info Center Host Printing Reference*. Host On-Demand includes a variety of PDF and Printer Definition Table (PDT) files contained in subdirectory:

```
C:\Program Files\IBM\HostOnDemand\HOD\pdfpdt
```

Host On-Demand cannot provide a PDF for every printer on the market. So, in many cases the administrator must chose an available PDF that comes closest to his printer type and edit it.

To explain how to change and to use a Printer Definition File, we changed the basic.pdf to work with the German DIN A4 paper format. The basic.pdf comes with Host On-Demand and has by default the American Letter format. We must open this PDF with an editor, change it as needed, and save it. Then we must use the Printer Definition Table Compiler to create a binary Printer Definition Table that is readable by Host On-Demand. This PDT must be placed in the subdirectory:

```
C:\Program Files\IBM\HostOnDemand\HOD\pdfpdt\usrpdf
```

The compiler automatically updates the index file. All files contained in the subdirectory are seen by the users who use the drop down box for selecting a PDT.

21.11.1 Example

We first use an editor such as Notepad to change the PDF. The PDF is the editable part of the PDF/PDT pair of files. The default location for Host On-Demand is:

```
C:\Program Files\IBM\HostOnDemand\HOD\pdfpdt
```

PDF files have all have similar structures: Depending on the printer capabilities, they may be more or less extensive:

- Macro area: Each line contains a three-character mnemonic, which is set equal to an escape sequence or command as understood by that printer type. The mnemonic can be easily remembered, and it is easier to use them further down in the PDF during editing. A comment may follow.

  Example:

  ```
  FFF EQU OC             /* Form Feed                                     */
  ```

- Session parameters: These contain items, for example, the page length, which is used for formatting on each page during that print job.

  Example:

  ```
  MAXIMUM_PAGE_LENGTH=060             /* Printed lines per page         */
  ```

- Control codes: These are sent to the printer when the equivalent command is contained in the data stream. For example, when the “end bracket” is encountered in the data stream Host On-Demand recognizes that as an END_JOB, and the codes defined for that are sent to the printer:

  Example:

  ```
  End_JOB= FFF
  ```

  This would send a form feed to the printer after each job to make sure the next print job starts at the top of a new page.

- Character Codes: If Host On-Demand encounters the character send by host it sends the appropriate code to the printer.

  Example:

  ```
  ASTERISK = 2A
  ```

We use Notepad to open the basic.pdf file located in C:\Program Files\IBM\HostOnDemand\HOD\pdfpdt.

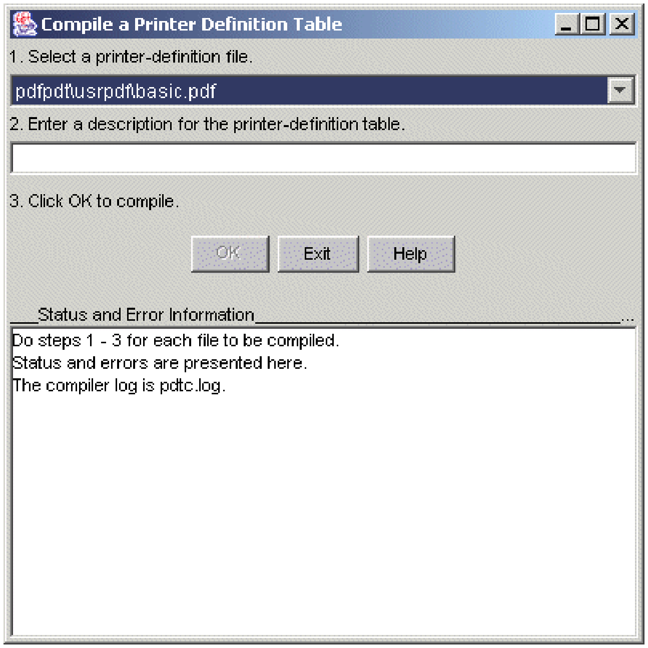
Now we change in the session parameter section the Maximum_Page_Length from the default = letter (60 LPP) to DIN A4 (72 LPP):

```
MAXIMUM_PAGE_LENGTH=072 /* Printed lines per page        */
```

We save this file to the subdirectory `C:\Program Files\IBM\HostOnDemand\HOD\pdfpdt\usrpdf`.

This PDF file must be compiled into a binary PDT. We start the Printer Definition Table Compiler by clicking at the Windows task bar **Start -> Programs -> IBM WebSphere Host On-Demand -> Administration -> Printer Definition Table Compiler**.

The window as shown in Figure 21-36 is displayed.



Compile a Printer Definition Table

1. Select a printer-definition file.

pdfpdt\usrpdf\basic.pdf

2. Enter a description for the printer-definition table.

3. Click OK to compile.

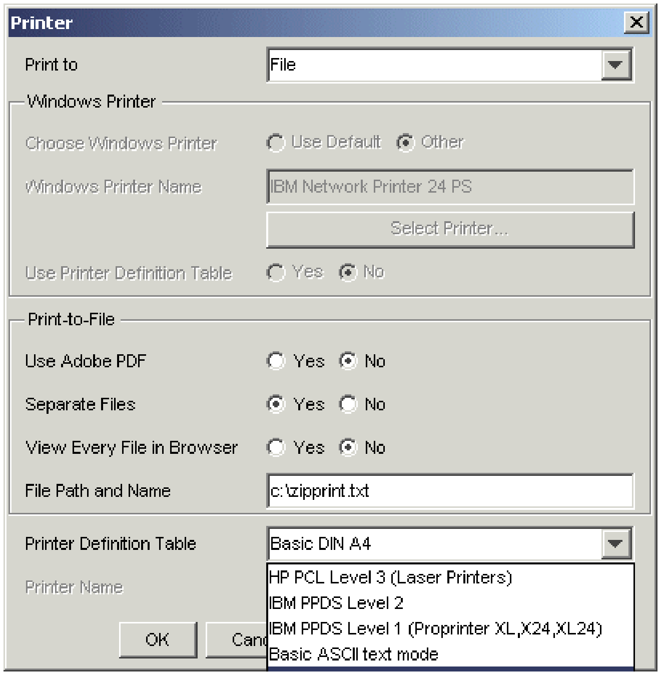
Do steps 1 - 3 for each file to be compiled.
Status and errors are presented here.
The compiler log is pdtc.log.

Figure 21-36 PDT compiler

By default there are no PDF files in the ..\usrpdf\ subdirectory. The compiler finds only the one that we just have copied.

A description may be filled in. Click **OK**.

The compiler will convert the PDF to a USR*name*.HODPDT where *name* is the file name of our PDF. In our example it places USRbasic.HODPDT into the subdirectory C:\Program Files\IBM\HostOnDemand\HOD\pdfpdt. The index file index.ndx is updated with the new additional PDT file pointer. When using the printer setup the next time, we can use this new PDT as shown in Figure 21-37.



Printer

Print to: File

Windows Printer

Choose Windows Printer ○ Use Default ● Other

Windows Printer Name: IBM Network Printer 24 PS

Select Printer...

Use Printer Definition Table ○ Yes ● No

Print-to-File

Use Adobe PDF ○ Yes ● No

Separate Files ● Yes ○ No

View Every File in Browser ○ Yes ● No

File Path and Name: c:\zipprint.txt

Printer Definition Table: Basic DIN A4

HP PCL Level 3 (Laser Printers)
IBM PPDS Level 2
IBM PPDS Level 1 (Proprinter XL,X24,XL24)
Basic ASCII text mode

Printer Name

OK Canc

Figure 21-37 Printer setup showing new PDT file

In Personal Communications, the user has control over editing and compiling of PDFs. However, in Host On-Demand only administrators can provide PDTs for the users. The Host On-Demand users do not have adequate access to the Host On-Demand server for PDF/PDT handling.

22

Macro support

Host On-Demand supports the creation of Macros to perform certain automated or repetitive tasks during the life of a host session. In this chapter we cover basic Macro support.

Host On-Demand V8 includes a new macro programming guide. It is available in multiple locations and formats:

- In the InfoCenter installed with Host On-Demand. In the Windows environment, Click **Start -> Programs -> IBM Host On-Demand -> InfoCenter -> Macro Programming Guide.**
- On the Host On-Demand distribution CD:

  ```
  file:///[cddrive]:/doc/[language]/doc/macro/macro.html
  file:///[cddrive]:/doc/[language]/doc/macro/macro.pdf
  ```

- The programming guide is also available as *IBM WebSphere Host On-Demand V8 Host On-Demand Macro Programming Guide*, SC31-6378.
- Installed on disk:

  ```
  [install directory]/HOD/[language]/doc/macro/macro.html
  [install directory]/HOD/[language]/doc/macro/macro.pdf
  ```

22.1 Macros

The Macro feature of Host On-Demand allows you to build scripts (Macros) consisting of command sequences that perform actions on the host. If you regularly do the same task when you work with a host system, you can record your keystrokes and the host's reactions, save them, and then play the Macro whenever you need to perform the same task. This is an ideal way to store frequently used actions for repeated use.

Macros are stored using XML script and are stored with the icon that launched the session. Multiple different Macros may be recorded and saved for a Host On-Demand session. However, remember that each Macro is downloaded when you start the session to which it applies.

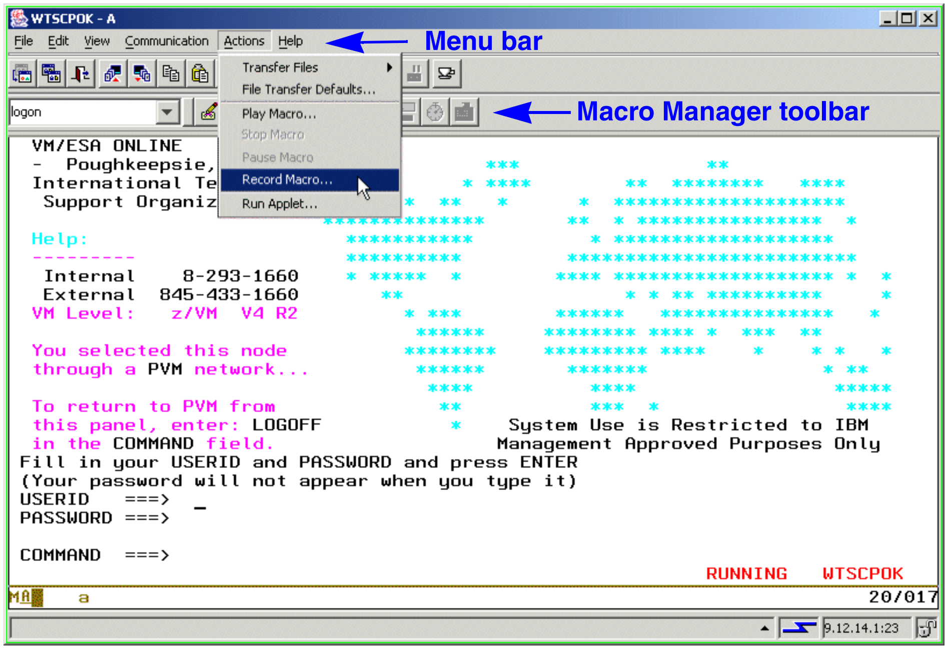
22.2 Creating and editing Macros

Macros may be recorded in two ways (see Figure 22-1):

- Using the **Actions-> Record Macro...** pull-down on the menu bar.
- Using the **Record macro** button on the Macro Manager toolbar. The Macro Manager gives you advanced Macro editing capability including:
  - Smart waits, which causes a macro to wait during playback until it recognizes a screen according to set conditions.
  - Prompts that allow you to type in information that varies, or which you do not want displayed during playback.
  - Data extraction that will retrieve data from a host application and put it into an applet or graphical user interface by using the MacroExtractEvent method of HACL. A Macro with data extraction in it is particularly useful for application developers who want to retrieve data from the host without knowing the structure. The data extraction function has no significance with regard to playback through a Host On-Demand emulator.

22.2.1 Recording a simple Macro

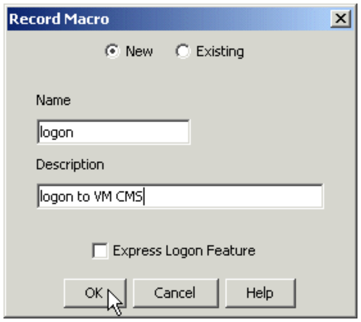
Let us record a Macro that simply logs onto your host VM session and opens a list of files.



```
 VM/ESA ONLINE
 -  Poughkeepsie,
 International Te
  Support Organiz

 Help:
 ---------
  Internal     8-293-1660
  External   845-433-1660
 VM Level:    z/VM   V4 R2

 You selected this node
 through a PVM network...

 To return to PVM from
 this panel, enter: LOGOFF              System Use is Restricted to IBM
 in the COMMAND field.                 Management Approved Purposes Only
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>  _
PASSWORD ===>

COMMAND  ===>
                                                   RUNNING   WTSCPOK
```

Figure 22-1 Begin recording a Macro

1. Click **Actions -> Record Macro**. See Figure 22-1. The following window will be displayed.



● New ○ Existing

Name

logon

Description

logon to VM CMS

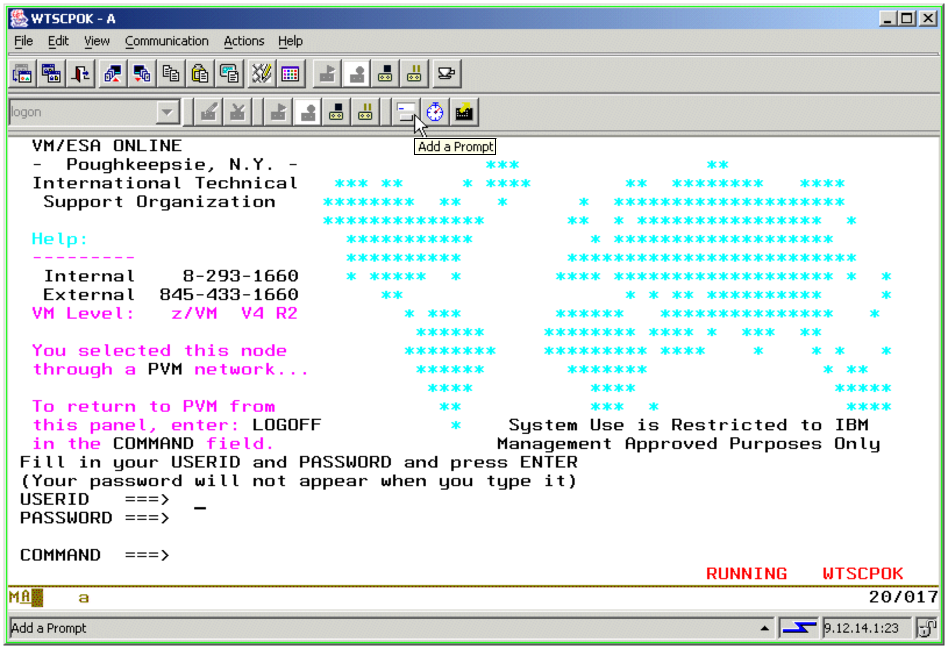
☐ Express Logon Feature

Figure 22-2 Record macro window

2. Select **New** and enter a name to identify the Macro for later use. Optionally, type a description. This is useful when you have more than one Macro; it can help to remind you what the Macro is used for. Select **Certificate Express Logon** if you are recording a Macro to use the Certificate Express Logon. To use this feature, the session must be an SSL session and using client authentication. The Certificate Express Logon option allows you to use the

client certificate for obtaining the user ID and password. It requires additional configuration on the Telnet servers. Refer to 15.2, “Certificate Express Logon” on page 580 for more details. Click **OK**.

3. You can insert one or more prompts in a Macro so that during playback, you can type information that varies or that you do not want to have displayed. During playback, a window opens so that you can enter the information which is then sent to the host application. By default, you are asked to respond to all the prompts in a single window when playback starts, but a checkbox in the Edit panel lets you ask to have the prompts appear at the appropriate places in sequence. We will add a prompt to the Macro requesting a VM user ID.



```
  VM/ESA ONLINE
  -  Poughkeepsie, N.Y. -
  International Technical
   Support Organization

  Help:
  ---------
   Internal     8-293-1660
   External   845-433-1660
  VM Level:    z/VM  V4 R2

  You selected this node
  through a PVM network...

  To return to PVM from
  this panel, enter: LOGOFF                System Use is Restricted to IBM
  in the COMMAND field.                  Management Approved Purposes Only
 Fill in your USERID and PASSWORD and press ENTER
 (Your password will not appear when you type it)
 USERID   ===>  _
 PASSWORD ===>

 COMMAND  ===>
                                                            RUNNING    WTSCPOK
MA       a                                                             20/017
```

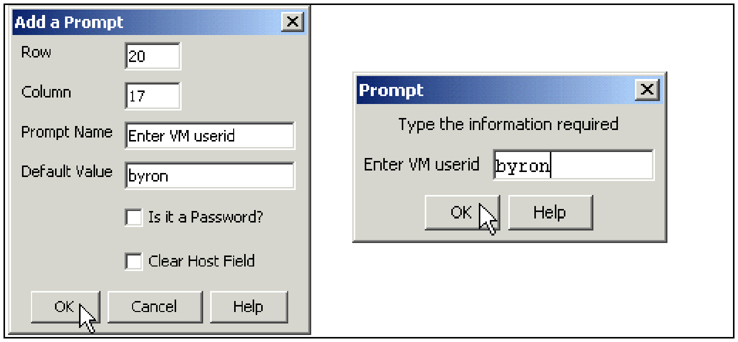
Figure 22-3 Adding a prompt to a Macro

4. Click the **Add a Prompt** button on the Macro Manager toolbar to add a prompt. See Figure 22-3.

5. The prompt panel shown on the left side of Figure 22-4 will be displayed. There are several points worth mentioning about the prompt panels shown in Figure 22-4:

   – The Row and Column fields indicate the position of the cursor when you clicked the **Prompt** button during recording. Your response to the prompt during playback will be entered at that position unless you change it. Unless there is a good reason, you should not do so because the host application will probably fail.

- If your response to the prompt will often be the same, you might want to enter a Default Value; you will still be prompted during playback and will be able to change the value, but you will often need only to click **OK.**
- If you check the **Is it a Password?** box, your response to the prompt will be displayed as asterisks and will be encrypted when the Macro is saved. Of course, this is not restricted to passwords.
- Some host applications put data into fields automatically, which means that a field that you are expecting to fill in from a prompt may already have something in it. If such a field is not cleared, invalid characters might be added to those that you enter. If you check the **Clear Host Field** box, anything already in the field is removed before you are prompted.



Row: 20
Column: 17
Prompt Name: Enter VM userid
Default Value: byron
□ Is it a Password?
□ Clear Host Field

Type the information required
Enter VM userid: byron

Figure 22-4 Adding a prompt to a Macro

6. The prompt panel shown on the right side of Figure 22-4 will be displayed when the Macro is run.
7. Continue in the host session performing the tasks you want to record. Every key you press is recorded as part of the Macro. To press keys you do not want to be included in the Macro, click **Pause**. When you have finished, click **Pause** again to continue. If you enter the wrong data while recording a Macro, you cannot go back to make corrections. You can, however, record over the existing Macro or edit the Macro code to make changes.
8. When your task is complete, click **Stop**. Recording stops and the Macro is saved. Macros are recorded using XML script (beginning in Version 4 of Host On-Demand). To make changes to the Macro use the Macro Manager (see 22.2.2, “Adding advanced functions to the simple Macro” on page 779). You can edit previous versions of Host On-Demand Macros using the Macro Editor. However, once you open a V3 Macro into the Macro Manager or Macro Editor, it is converted to the XML format. It cannot be converted back to the V3 format.

When we are finished, the Macro looks like Figure 22-1.

Example 22-1 Simple Host On-Demand Macro

```
<HAScript name="logon" description="logon to VM CMS" timeout="60000" pausetime="300"
promptall="true" author="" creationdate="" supressclearevents="false" usevars="false" >

<comment>
         Definition of the first screen. This is the initial logon screen.
</comment>
    <screen name="Screen1" entryscreen="true" exitscreen="false" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
        </description>
        <actions>
            <prompt name="Enter VM userid" description="" row="20" col="17" len="8"
default="byron" clearfield="false" encrypted="false" movecursor="true" xlatehostkeys="true"
assigntovar="" varupdateonly="false" />
            <input value="[tab]jnglrot[enter]" row="0" col="0" movecursor="true"
xlatehostkeys="true" encrypted="false" />
        </actions>
        <nextscreens timeout="0" >
            <nextscreen name="Screen2" />
        </nextscreens>
    </screen>

    <screen name="Screen2" entryscreen="false" exitscreen="false" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
            <numfields number="9" optional="false" invertmatch="false" />
            <numinputfields number="1" optional="false" invertmatch="false" />
        </description>
        <actions>
            <input value="[clear]" row="0" col="0" movecursor="true" xlatehostkeys="true"
encrypted="false" />
        </actions>
        <nextscreens timeout="0" >
            <nextscreen name="Screen3" />
        </nextscreens>
    </screen>

    <screen name="Screen3" entryscreen="false" exitscreen="false" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
            <numfields number="5" optional="false" invertmatch="false" />
            <numinputfields number="1" optional="false" invertmatch="false" />
        </description>
        <actions>
            <input value="[clear]" row="0" col="0" movecursor="true" xlatehostkeys="true"
encrypted="false" />
        </actions>
        <nextscreens timeout="0" >
            <nextscreen name="Screen4" />
        </nextscreens>
    </screen>

<comment>
         Definition of the last screen. It executes the fulist CMS command.
</comment>
<screen name="Screen4" entryscreen="false" exitscreen="true" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
            <numfields number="5" optional="false" invertmatch="false" />
            <numinputfields number="1" optional="false" invertmatch="false" />
        </description>
        <actions>
           <input value="fulist[enter]" row="0" col="0" movecursor="true" xlatehostkeys="true"
encrypted="false" />
        </actions>
        <nextscreens timeout="0" >
        </nextscreens>
    </screen>

</HAScript>
```

22.2.2 Adding advanced functions to the simple Macro

The Macro Editor allows you to expand a simple Macro to include advanced functions available in Host On-Demand such as:

- Variables
- Conditional if-else logic
- Macro Chaining
- Run programs from a Macro

All of these features of Macros are documented in the Host Access Beans documentation installed with the Host On-Demand Toolkit. *Appendix A. Macro Script Syntax* contains specifics on all the Macro commands and extensive examples of sophisticated Macros. The InfoCenter contains a tutorial on using the Macro Manager. The Host On-Demand InfoCenter is located at:

http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/

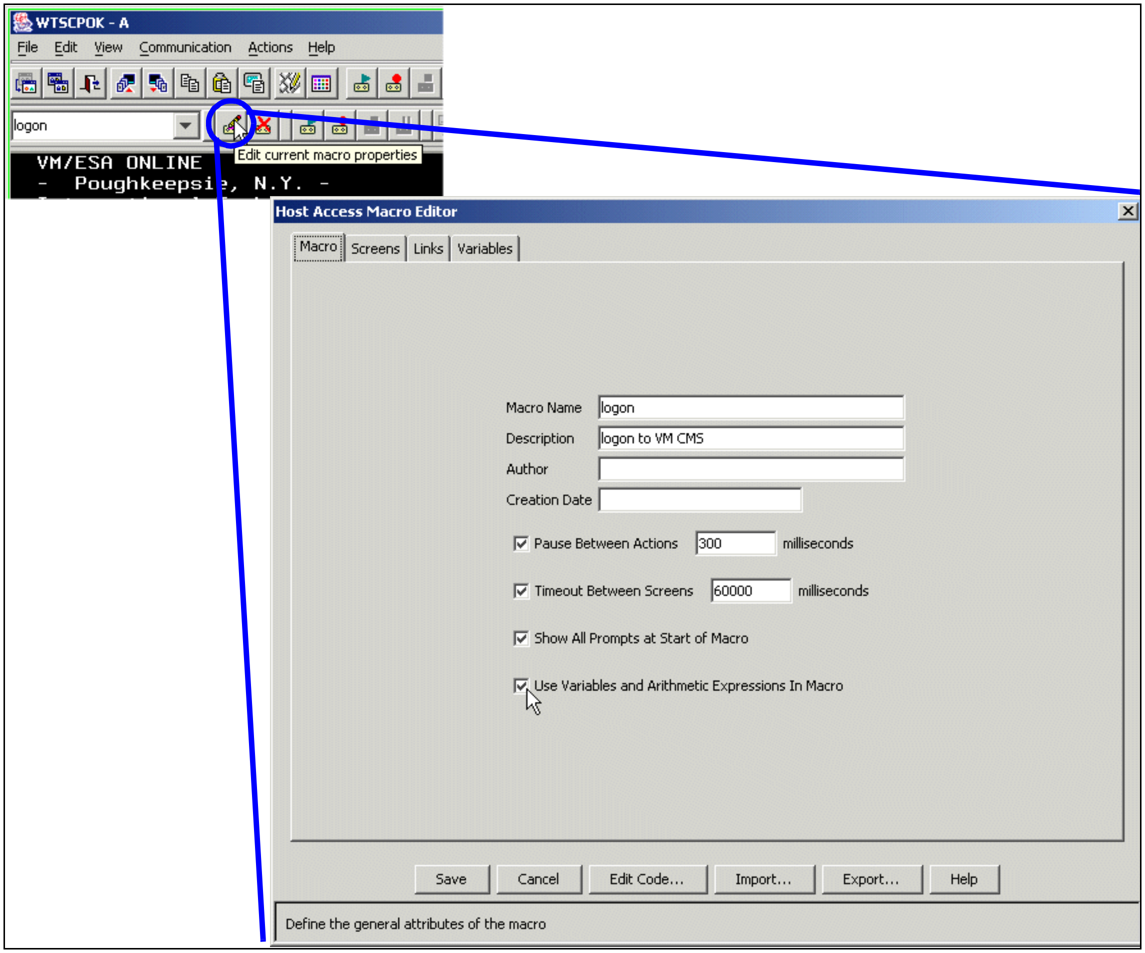
> **Important:** To enable the advanced Macro features, you must check the **Use Variables and Arithmetic Expressions in Macro** box on the main Macro Editor panel. See Figure 22-5.

Updating the Macro

We now return to the Host On-Demand session used to record the simple Macro and open the Macro Editor The simple Macro recorded earlier will be enhanced in the following ways:

- Define two variables to be used in the Macro processing
- Assign the user ID to one of the variables
- Execute an external program (Notepad) passing one of the variables to it. See Figure 22-8 on page 784.
- Read data from screen and display a message based on a conditional test of its value. See Figure 22-10 on page 786.

We invoked the Macro editor from the Macro Manager toolbar to make these updates to the Macro. See Figure 22-5 for details.



Macro Name: logon

Description: logon to VM CMS

Author:

Creation Date:

☑ Pause Between Actions 300 milliseconds

☑ Timeout Between Screens 60000 milliseconds

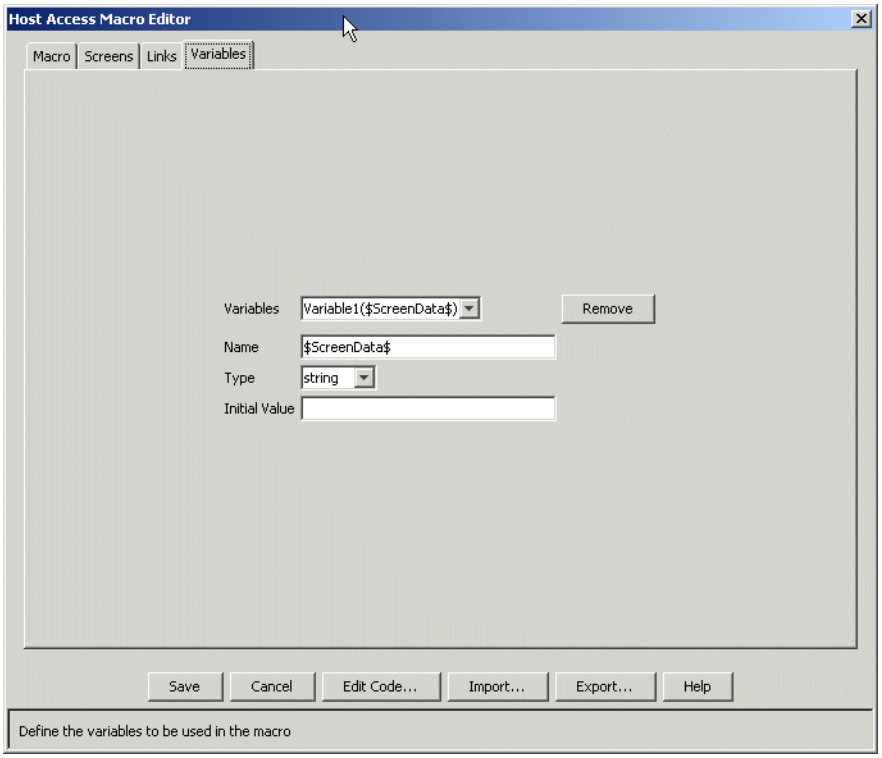
☑ Show All Prompts at Start of Macro

☑ Use Variables and Arithmetic Expressions In Macro

Define the general attributes of the macro

Figure 22-5 Invoking the Macro Manager

Our first task is to define two variables that we will use in the Macro. Selecting the **Variables** tab shown in Figure 22-5 displays the window shown in Figure 22-6.



Variables: Variable1($ScreenData$)

Name: $ScreenData$

Type: string

Initial Value:

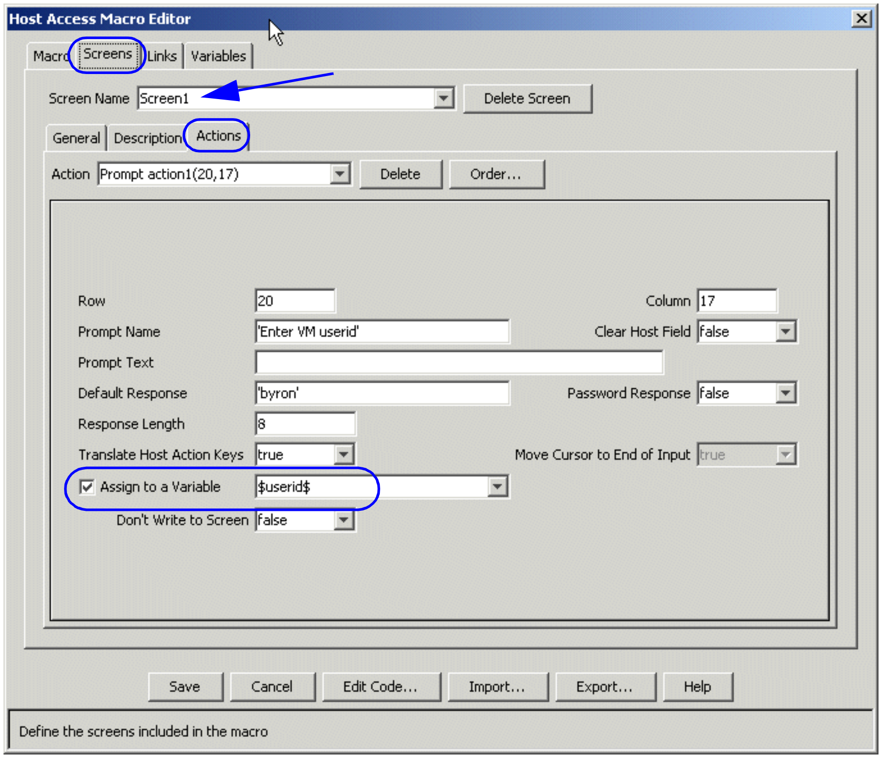
Define the variables to be used in the macro

Figure 22-6 Defining Macro variables

We used this window to define two variables ($ScreenData$ and $userid$) that will be used later on in the Macro.

The remaining additional functions were added to the simple Macro by accessing the **Actions** panel on the appropriate screen.

First, we assign the user ID entered in the Macro prompt (see Figure 22-4 on page 777) to the variable $userid$. Note from the Macro listing in Example 22-1 on page 778 that the Macro prompt action is on Screen1. Select the **Screen** tab on the Macro Editor panel to see the screen selections, then select **Screen1**.



Screen Name: Screen1

Action: Prompt action1(20,17)

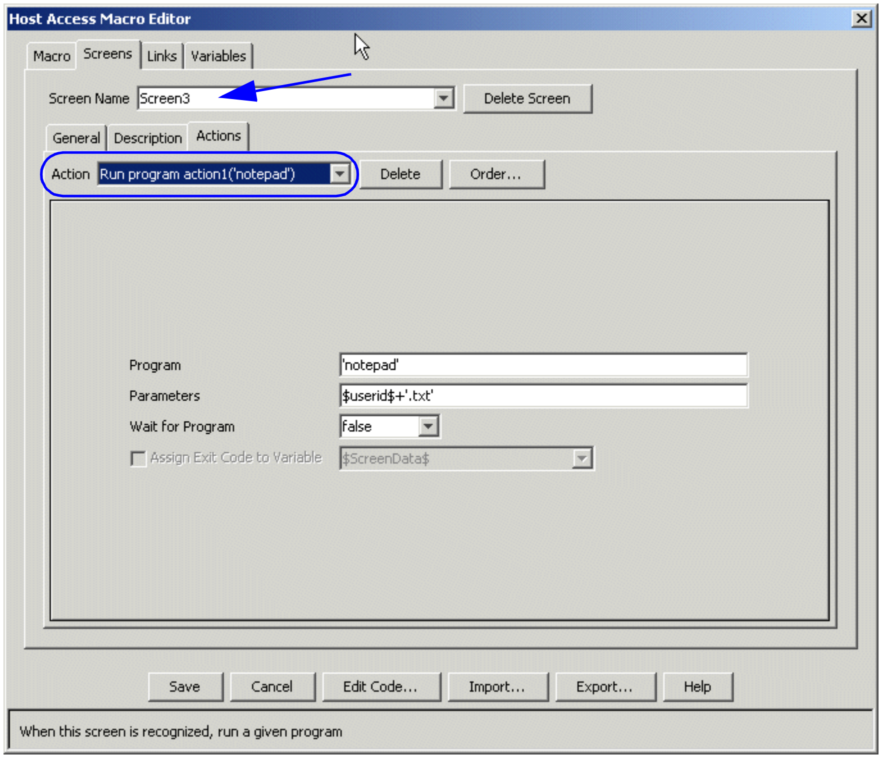
Row: 20
Column: 17
Prompt Name: 'Enter VM userid'
Clear Host Field: false
Prompt Text:
Default Response: 'byron'
Password Response: false
Response Length: 8
Translate Host Action Keys: true
Move Cursor to End of Input: true
☑ Assign to a Variable: $userid$
Don't Write to Screen: false

Define the screens included in the macro

Figure 22-7   Macro screens tab displaying Screen1

There are several items to note on Figure 22-7. The Macro screen to be manipulated is selected in the **Screen Name** field. We want to modify the actions taken on this screen, so we must select the **Actions** tab. Note the **Prompt Name** and **Default Response** fields. These fields were filled in when we initially recorded our Macro. To assign the value entered for VM user ID in the prompt to variable $userid$, all we must do is check the **Assign to a Variable** box and type in the variable name.

Next, we want to execute an external program using the variable we just captured. For our example, we will execute the Windows Notepad program passing it a filename of “$userid$.txt” to be edited. We chose to perform this action from Screen3, however, it could have been performed from any of the screens in the Macro. Select **Screen3** in the Screen Name field.



Screen Name Screen3

Action Run program action1('notepad')

Program 'notepad'

Parameters $userid$+'.txt'

Wait for Program false

□ Assign Exit Code to Variable $ScreenData$

When this screen is recognized, run a given program

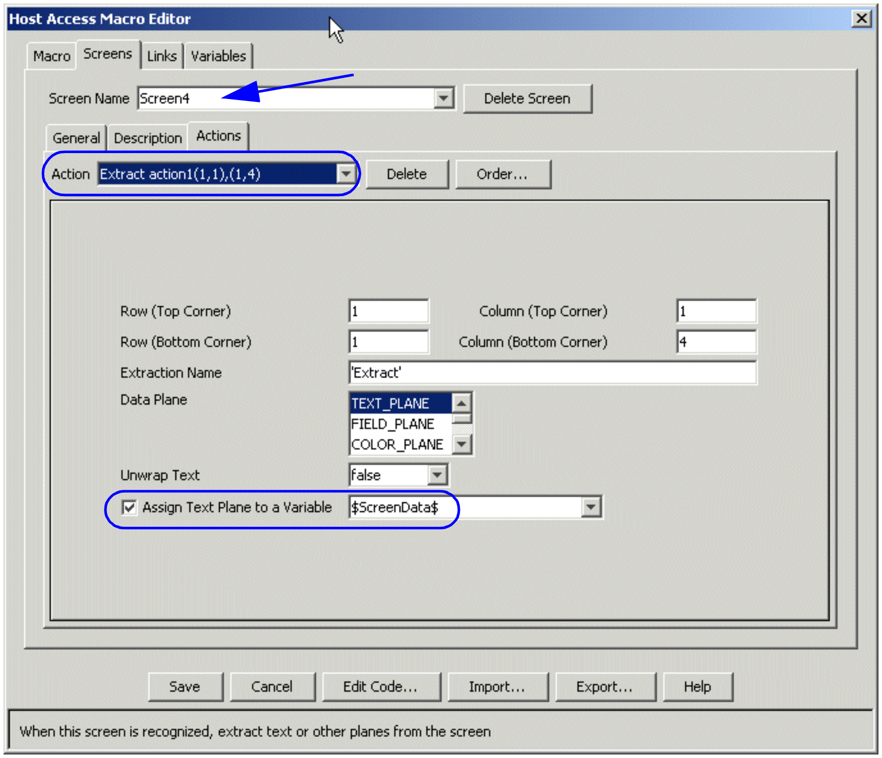
Figure 22-8 Execute Notepad from a Macro

In Figure 22-8, note that we have selected Screen3 to modify. In addition, we have selected **Run program action** from the Action pulldown list. When the **Run program action** is selected, the fields on the lower half of the panel are automatically displayed. Note that we selected **Notepad** as the program to be executed and “$userid$.txt” as the parameters to be passed to the program. When the Macro reaches Screen3 in its execution, a Notepad window will open up while the Macro continues execution.

Our last addition to the Macro is to read some data from the screen and display a conditional message based on the data read from the screen. We choose to perform these actions based on data read from Screen4. Note that we must perform two actions on Screen4:

- Read (extract) data from the screen and assign it to a variable ($ScreenData$)
- Display a message based on what data was read from the screen

Select **Screen4** in the Screen Name field.



Screen Name: Screen4

Action: Extract action1(1,1),(1,4)

Row (Top Corner)	1	Column (Top Corner)	1
Row (Bottom Corner)	1	Column (Bottom Corner)	4

Extraction Name: 'Extract'

Data Plane: TEXT_PLANE
FIELD_PLANE
COLOR_PLANE

Unwrap Text: false

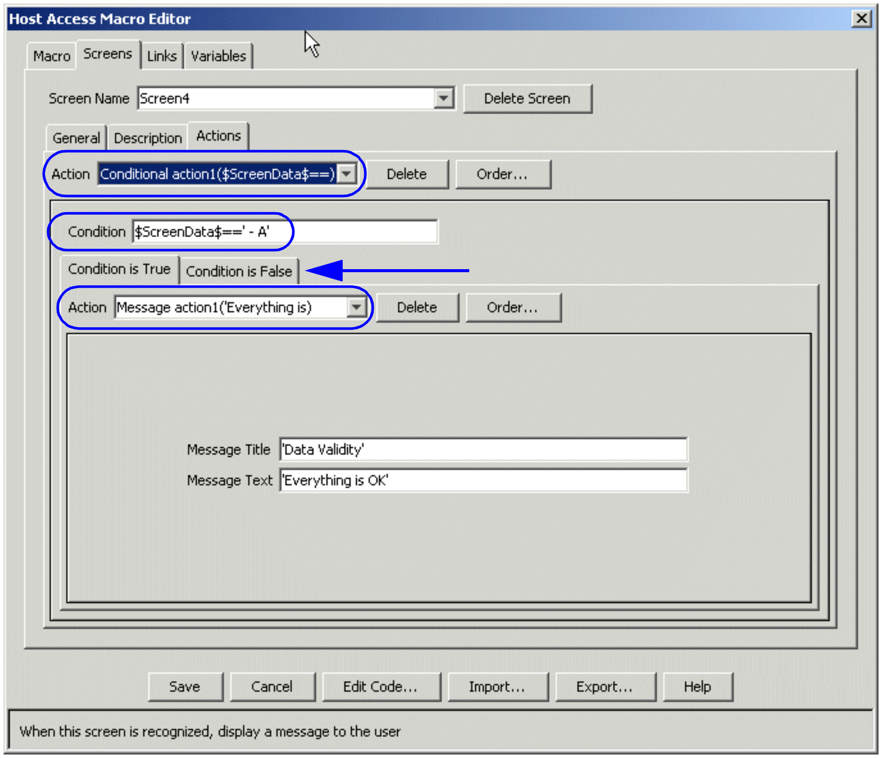
☑ Assign Text Plane to a Variable: $ScreenData$

When this screen is recognized, extract text or other planes from the screen

Figure 22-9 Extracting data from Screen4

The first action we perform on Screen4 is to extract a string of data from the screen and assign is to variable $ScreenData$. This is all easily performed with one Extract action as shown in Figure 22-9.

Next, we perform a conditional checking action on the data to decide which message to display.



Screen Name Screen4

Action Conditional action1($ScreenData$==)

Condition $ScreenData$==' - A'

Action Message action1('Everything is)

Message Title 'Data Validity'

Message Text 'Everything is OK'

When this screen is recognized, display a message to the user

Figure 22-10 Conditional checking and actions in the Macro

Everything required for the conditional checking and action to be taken is defined on this Conditional action window. Note that the **Action** is **“**`Conditional action`**”** and the condition to be checked is defined in the **Condition** field. Two conditional results must be defined (“True” and “False”), and an action to be taken for each result must be defined (second **Action** field on the panel). The fields on the lower half of the panel change based on what **Action** and **Condition** are selected.

Here is a listing for the updated Macro. Compare it with the Macro listed on Example 22-1.

Example 22-2 Simple HOD Macro enhanced

```
<HAScript name="logon" description="logon to VM CMS" timeout="60000" pausetime="300"
promptall="true" author="" creationdate="" supressclearevents="false" usevars="true" >

    <vars>
        <create name="$ScreenData$" type="string" value="" />
        <create name="$userid$" type="string" value="" />
    </vars>
```

```
<comment>
         Definition of the first screen. This is the initial logon screen.
</comment>
<screen name="Screen1" entryscreen="true" exitscreen="false" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
        </description>
        <actions>
           <prompt name="&apos;Enter VM userid&apos;" description="" row="20" col="17" len="8" 
default="&apos;jnglrot&apos;" clearfield="false" encrypted="false" movecursor="true" 
xlatehostkeys="true" assigntovar="$userid$" varupdateonly="false" />
            <input value="&apos;[tab]by07on[enter]&apos;" row="0" col="0" movecursor="true" 
xlatehostkeys="true" encrypted="false" />
        </actions>
        <nextscreens timeout="0" >
            <nextscreen name="Screen2" />
        </nextscreens>
    </screen>

    <screen name="Screen2" entryscreen="false" exitscreen="false" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
            <numfields number="9" optional="false" invertmatch="false" />
            <numinputfields number="1" optional="false" invertmatch="false" />
        </description>
        <actions>
            <pause value="500" />
            <input value="&apos;[clear]&apos;" row="0" col="0" movecursor="true" 
xlatehostkeys="true" encrypted="false" />
        </actions>
        <nextscreens timeout="0" >
            <nextscreen name="Screen3" />
        </nextscreens>
    </screen>

    <screen name="Screen3" entryscreen="false" exitscreen="false" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
            <numfields number="5" optional="false" invertmatch="false" />
            <numinputfields number="1" optional="false" invertmatch="false" />
        </description>
        <actions>
            <pause value="500" />
            <input value="&apos;[clear]&apos;" row="0" col="0" movecursor="true" 
xlatehostkeys="true" encrypted="false" />
            <runprogram exe="&apos;notepad&apos;" param="$userid$+&apos;.txt&apos;" 
wait="false" assignexitvalue="" />
        </actions>
        <nextscreens timeout="0" >
```

```
            <nextscreen name="Screen4" />
        </nextscreens>
    </screen>

<comment>
         Definition of the last screen. It executes the fulist CMS command.
</comment>
<screen name="Screen4" entryscreen="false" exitscreen="true" transient="false">
        <description>
            <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
            <numfields number="5" optional="false" invertmatch="false" />
            <numinputfields number="1" optional="false" invertmatch="false" />
        </description>
        <actions>
            <pause value="500" />
            <input value="&apos;fulist[enter]&apos;" row="0" col="0" movecursor="true"
xlatehostkeys="true" encrypted="false" />
            <extract name="&apos;Extract&apos;" planetype="TEXT_PLANE" srow="1" scol="1"
erow="1" ecol="4" unwrap="false" assigntovar="$ScreenData$" />
            <message title="&apos;data read&apos;" value="$ScreenData$" />
            <if condition="$ScreenData$==&apos; - A&apos;" >
                  <message title="&apos;Data Validity&apos;" value="&apos;Everything is
OK&apos;" />
            </if>
            <else>
                  <message title="&apos;Data Validity&apos;" value="&apos;Everything is
BAD&apos;" />
            </else>
        </actions>
        <nextscreens timeout="0" >
        </nextscreens>
    </screen>

</HAScript>
```

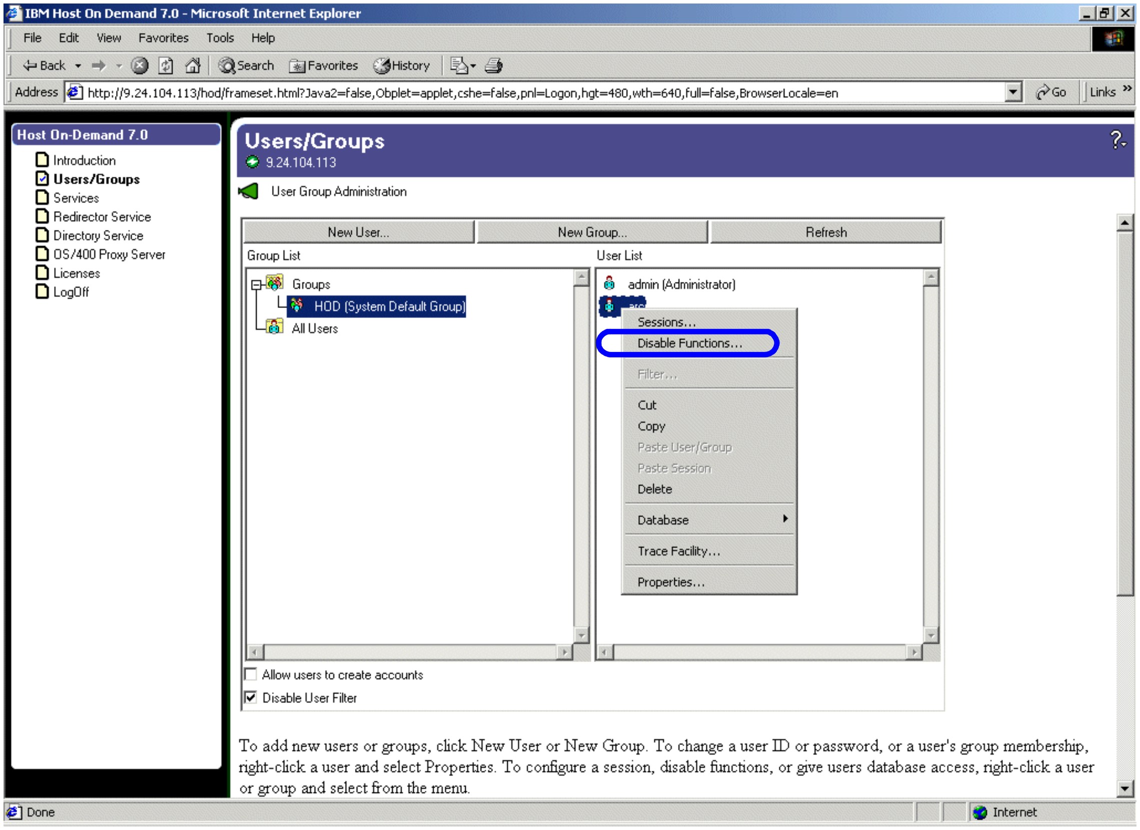
22.3 HOD administrators and Macros

User access to Host On-Demand functions is controlled by the Host On-Demand administrator. The administrator determines which HOD groups, users, or emulator sessions are enabled or disabled for the appropriate Host On-Demand functions. The Host On-Demand administrative interface is generally the way user access to Macro functionality is set.

> **Note:** You can use a Macro with every session that is launched from the same icon, but not with sessions launched from other icons (unless they are copies of the original session made after the Macro was recorded).
>
> You can save as many Macros as you want, but remember that if your configuration model is to save preferences on the HOD server, then all the macros will be downloaded when you start the session in which they were recorded.

22.3.1 Controlling access to HOD Macros

By default all users have access to all Host On-Demand Macro functions.The Host On-Demand administrator can disable various HOD functions by selecting **Users/Groups** then right-clicking the group, user, or session for which they wish to limit access to HOD functions. Refer to Figure 22-11.



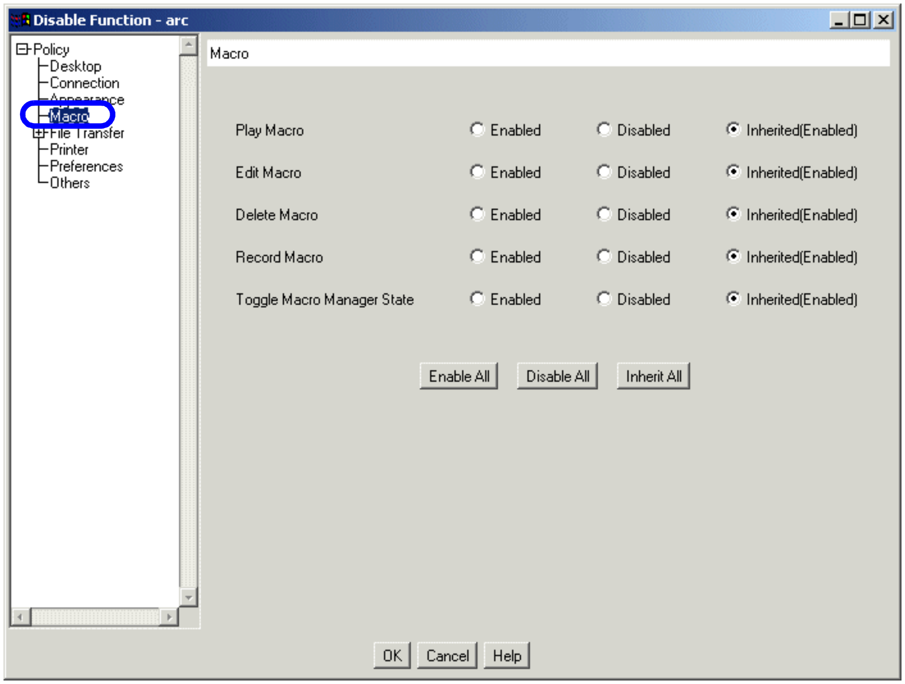
http://9.24.104.113/hod/frameset.html?Java2=false,Obplet=applet,cshe=false,pnl=Logon,hgt=480,wth=640,full=false,BrowserLocale=en

☐ Allow users to create accounts

☑ Disable User Filter

To add new users or groups, click New User or New Group. To change a user ID or password, or a user's group membership, right-click a user and select Properties. To configure a session, disable functions, or give users database access, right-click a user or group and select from the menu.

Figure 22-11 Disabling access to HOD Functions



Macro

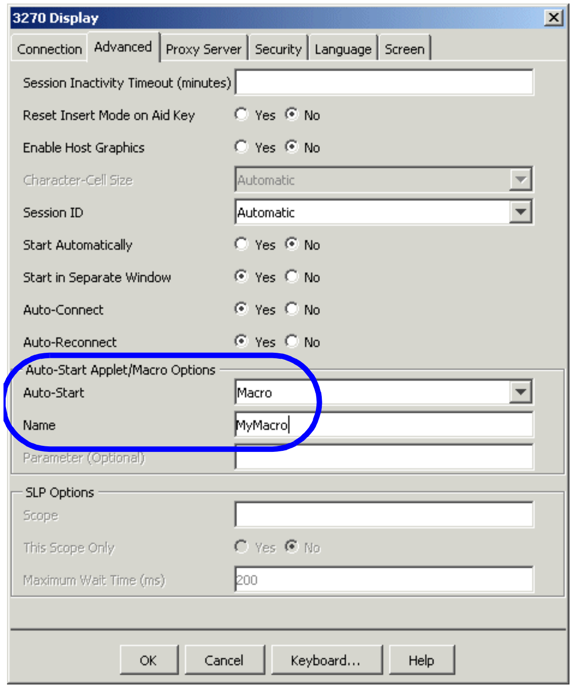
Play Macro	○ Enabled	○ Disabled	● Inherited(Enabled)
Edit Macro	○ Enabled	○ Disabled	● Inherited(Enabled)
Delete Macro	○ Enabled	○ Disabled	● Inherited(Enabled)
Record Macro	○ Enabled	○ Disabled	● Inherited(Enabled)
Toggle Macro Manager State	○ Enabled	○ Disabled	● Inherited(Enabled)

Figure 22-12 Disabling specific Macro functions

On the Disable Function panel, select **Macro** from the selection tree on the left panel, then enable or disable the various Macro functions as required. Refer to Figure 22-12.

22.3.2 Automatically starting Macros

The administrator, or a user with appropriate authorities, can set the properties on a HOD session to automatically execute a Macro when the session is started. Configuring a session to AutoStart a Macro is done by right-clicking the HOD session and selecting **Properties**. Next, select the **Advanced property** page for the session, and enter the name of the HOD Macro you want to Autostart in the AutoStart Applet/Macro options field as shown in Figure 22-13.



Session Inactivity Timeout (minutes)

Reset Insert Mode on Aid Key ○ Yes ● No

Enable Host Graphics ○ Yes ● No

Character-Cell Size: Automatic

Session ID: Automatic

Start Automatically ○ Yes ● No

Start in Separate Window ● Yes ○ No

Auto-Connect ● Yes ○ No

Auto-Reconnect ● Yes ○ No

Auto-Start Applet/Macro Options

Auto-Start: Macro

Name: MyMacro

Parameter (Optional)

SLP Options

Scope

This Scope Only ○ Yes ● No

Maximum Wait Time (ms): 200

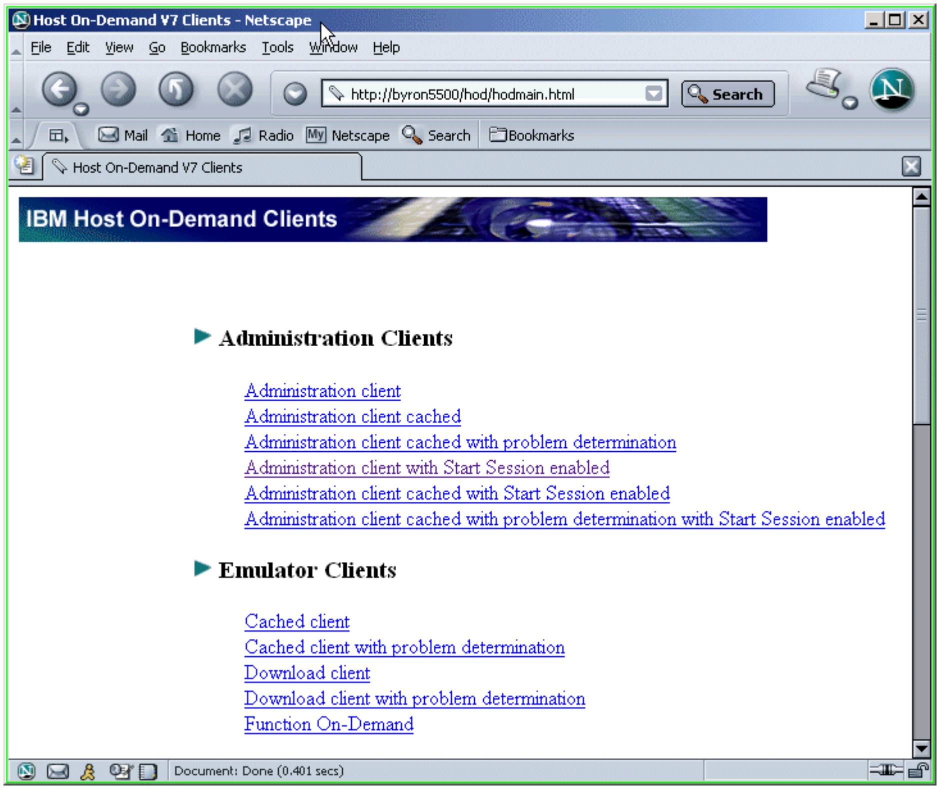
Figure 22-13 Setting a Macro to auto-start with the session

22.4 Deploying Macros

The following sections describe the process of deploying Macros based on the Deployment Wizard model used to create the session.

22.4.1 Setting up Macros for Configuration Server or combined model

The Host On-Demand administrator may record and assign a Macro to a session or user ID. The Macro is saved in the user's account file (HOD.user_id).user. Host On-Demand administrators must start the emulator session from the Admin Console, create a new Macro, or import an existing Macro, and save the Macro under the session icon. The administrator should use the HOD Admin client that has **Start Session Enabled**.


Host On-Demand V7 Clients - Netscape
File Edit View Go Bookmarks Tools Window Help
http://byron5500/hod/hodmain.html
Search
Mail Home Radio Netscape Search Bookmarks
Host On-Demand V7 Clients
Document: Done (0.401 secs)

IBM Host On-Demand Clients

▶ Administration Clients

- Administration client
- Administration client cached
- Administration client cached with problem determination
- Administration client with Start Session enabled
- Administration client cached with Start Session enabled
- Administration client cached with problem determination with Start Session enabled

▶ Emulator Clients

- Cached client
- Cached client with problem determination
- Download client
- Download client with problem determination
- Function On-Demand

Figure 22-14 Administrator setting up a global Macro

Once you log on using the correct Administration client, you can start the session and record a Macro.

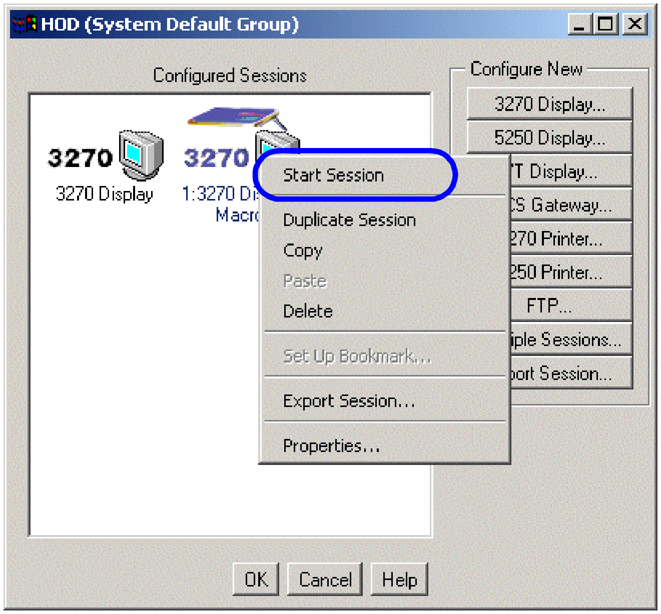


Figure 22-15 Recording a Macro for a specific session

Right-click the session icon and then select **Start the session**. Once the session is started you simply record the Macro. See Figure 22-15.

22.4.2 Deploying Macros for the Configuration Server model

Tip: If your users are not allowed to save individual preferences, then users will not be able to save any Macros.

It is quite probable that at some point after running HOD for a bit, you find some user has built a sophisticated Macro that would be useful for other users. To make a macro written by a user to other HOD users is quite simple:

- Since you are using the Configuration Server model, all the user configuration information including Macros is stored on the HOD server:
  - In this situation the HOD administrator may choose to log on to the HOD server using the user Id and password of the user with the interesting Macro. Once logged on, use the Macro Manager to export the Macro to a file.
  - If you do not want to log on to the users HOD session, then ask the user to export the Macro using the MacroManager interface.

- With the Macro now in hand, you can deploy the Macro to other users; see Chapter 22.4.1, “Setting up Macros for Configuration Server or combined model” on page 792.

22.4.3 Setting up Macros for HTML-based server model

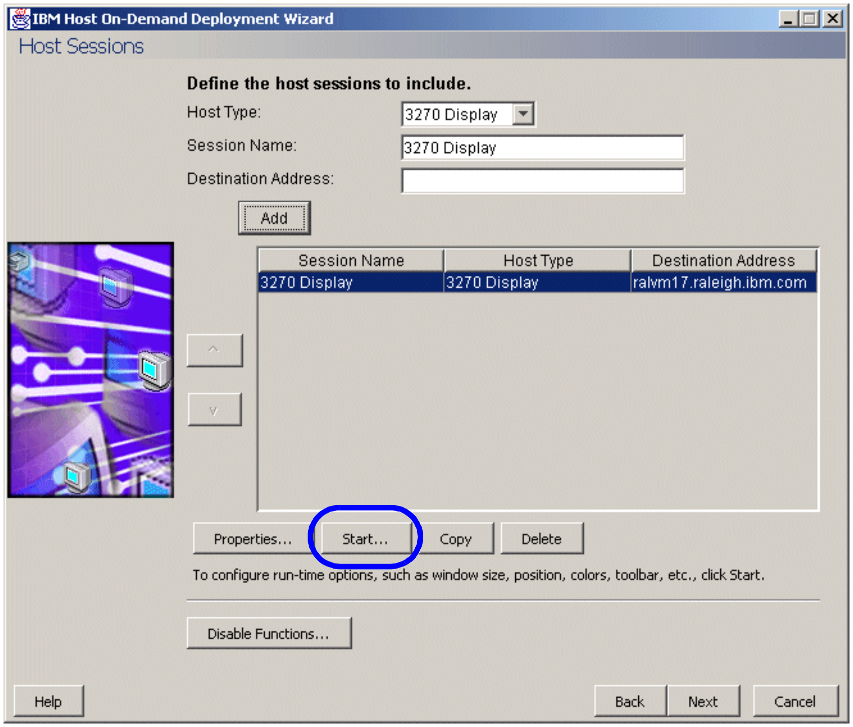
The Host On-Demand administrator can very easily deploy Macros when using the Deployment Wizard to build client code based on the HTML model. Since this model does not store user configuration information on the HOD server, the Macros must be defined when:

- Running the Deployment Wizard

or

- Exporting the Macro, sending to users and asking them to import the Macro

Using the Deployment Wizard on the screen that allows you to add the host session type, select **Start Session**. Once the session is started, simply record the Macro or import an existing Macro. Finish running the Deployment Wizard, and once the files are deployed on the Web server, all users accessing them will be able to use the Macro(s) you have defined.



IBM Host On-Demand Deployment Wizard

Host Sessions

Define the host sessions to include.

Host Type: 3270 Display

Session Name: 3270 Display

Destination Address:

Session Name	Host Type	Destination Address
3270 Display	3270 Display	ralvm17.raleigh.ibm.com

To configure run-time options, such as window size, position, colors, toolbar, etc., click Start.

Figure 22-16 Deployment Wizard and starting session to add a Macro

22.4.4 Deploying Macros for HTML model and combined model

It is quite probable that at some point after running HOD for a bit, you find some user has built a sophisticated Macro that would be useful for other users. Have the user with the interesting Macro use the MacroManager to export the Macro to a file.

If the users you will deploy the Macro to are using the Combined Server Model then refer to Chapter 22.4.1, “Setting up Macros for Configuration Server or combined model” on page 792.

For users running the HTML Model you have two options:

- Allow other users access to the Macro by sending to them through e-mail, or placing on some location like a network drive for them to access
- Rerun the Deployment Wizard and on the page where the session is defined you must:
  - Start the session.

  - Start the Macro Manager and import the Macro.
  - Redeploy the HTML generated by the Deployment Wizard to your Web server and now your users will have access to the new Macro.

22.5 When problems occur with HOD Macros

A Macro is a sequence of instructions that allow you to navigate through some number of host screens. If you are not thorough and complete when defining each individual screen, and *every* possible screen that can follow it, you will experience problems.

For instance, if a screen is matched too early, then it is quite possible that the entire logic flow of the Macro will be disrupted. Once a screen is matched prematurely, then it is almost certain that the logic that follows this screen will be out of sync.

22.5.1 Causes of screen mismatches or non-matches

During initial screen recognition, when the Macro is first recorded Macro uses OIA status and the number of fields on a screen to determine Screen recognition. If a situation occurs where the screens that follow a recognized screen change, and are no longer uniquely defined by their OIA status and field count, it is possible for Macro processing to think it is on the wrong next screen, that is, a screen mismatch. If the flow of screen information from the host changes, it can also cause a screen mismatch. A screen match based simply on OIA status and field counts is not always sufficient.

There are multiple reasons for screen mismatches and timeouts

- Timing Problems caused by network and host delays

  To slow down Macro execution use the Macro manager, add either a global pause for all Macros or add a Screen pause on a particular screen you are having problems with. Pauses will certainly resolve the problem of potential screen mismatches, but will also increase the amount of time it takes to run through a Macro. See 22.5.3, “Adding pauses” on page 798, and 22.5.4, “Adding timeouts” on page 799.

- Transient screens appearing during normal Macro processing

  Unexpected screens from host may occur because of the occurrence of some transient screen appearances, such as an operator message popup. See 22.5.6, “Unexpected screens from the host” on page 801.

- Multiple possible different text phrases on a screen

Defining the logic for what appears on a screen can be complicated, but HOD Macro gives you several options:

   - If there are occasions where the current screen may occasionally have some new text on it that indicates you should move to the next Screen, try using the Optional screen descriptor. See Chapter 22.5.2, "Optional field" on page 798.
   - You may also have a screen that you define not by what the screen displays, but what it does not. For this situation using the Inverse Descriptor may work best. See Chapter 22.5.5, "Use of inverse Descriptor" on page 800.

- Host Screens being sent in multiple blocks of data

  For situations where the screen data is sent in blocks, the screen will be updated as the separate portions of the screen are received. During this screen update the HOD Macro processing may recognize the half written screen in error. To fix this, you may wish to add additional fields to the screen description. A field that occurs in the top portion of the screen and one that appears in the lower portion of the screen is normally sufficient to ensure the entire screen has arrived.

- Next Screens with same number of Fields and OIA Status

  The screens that follow a recognized screen (that is, the Next Screen) may not always have a unique OIA and field Count value that tells them apart. Using the MacroManager, add additional fields to the Screen Descriptions for the screens in question. You may find that simply adding:

   - The cursor position
   - Screen attribute, see Chapter 22.5.7, "Screen attributes" on page 803
   - Additional text string
   - Additional fields as described in step 3 above
   - To the screen description resolves all your problems.

9. Host Screen changes by the addition of an item in a list of items

   The easiest way to handle situations where lists of host data may change is to add looping into the HOD Macro logic. See 22.5.8, "Screen scroll problems - adding looping to Macro" on page 803.

You may ultimately need to debug some problems by adding trace statements in the Macro. See 22.6.1, "Adding trace statements to Macros" on page 805.

22.5.2 Optional field

For every screen definition there is an Optional screen descriptor field. When a descriptor is defined as optional, it is used for screen matching when all the non-optional descriptors have been checked but have *failed* to match. This can be useful concept when a screen has the possibility of containing multiple field possibilities that still require you to move onto the next screen.

For instance, you may have a screen that displays the text RUNNING in the lower right portion of the screen. On occasion this screen may display CONNECTED rather then RUNNING. This is where using the Optional field descriptor may be useful. The Optional descriptor configures the screen recognition logic to recognize the screen if the text expected on a screen exists or when the Optional descriptor is present.

Example 22-3 Logic flow of Optional text field

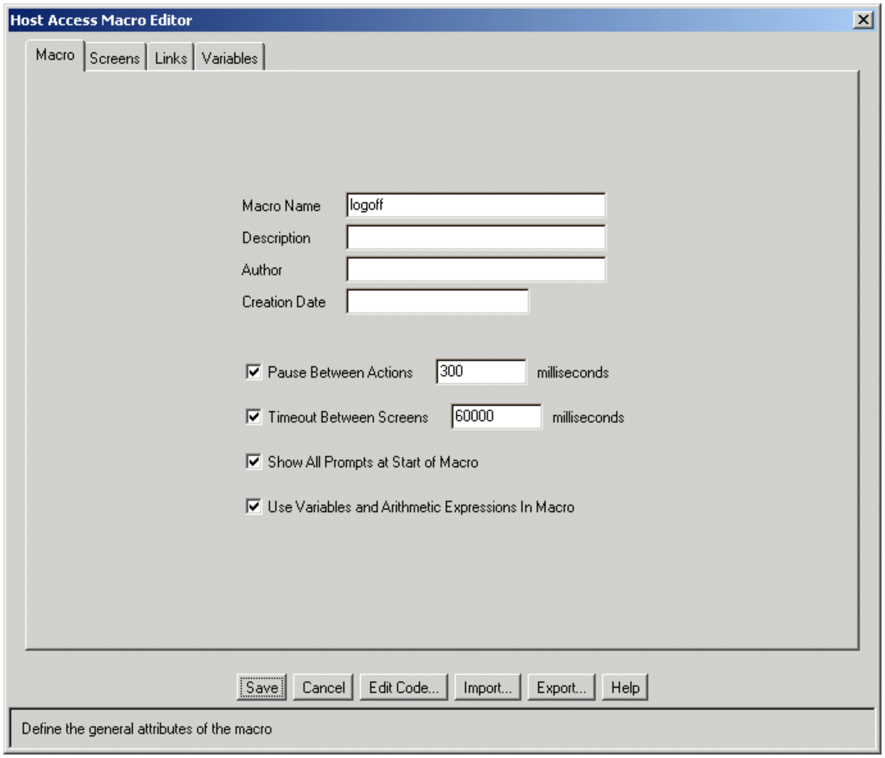
```
If text on screen exists then
   screen match /* screen has Running */
else
      if optional field exists then
         screen match /* screen displays CONNECTED */
else
   no match
```

22.5.3 Adding pauses

The pause time can be set per screen or globally for the Macro. The pause time is defined as the time to wait between actions on a screen once a screen has been displayed. Increase this time to allow for possible performance problems that may occur during interactions with the host.

22.5.4 Adding timeouts

The timeout value in milliseconds determines how long the Macro will wait to match a screen before timing out. If the timeout value is not long enough then it is possible for the Macro to timeout and stop executing before the host screen becomes available. Timeout value in the Macro can be set for an individual screen or globally. Refer to Figure 22-17.



Macro Name: logoff
Description:
Author:
Creation Date:

☑ Pause Between Actions 300 milliseconds

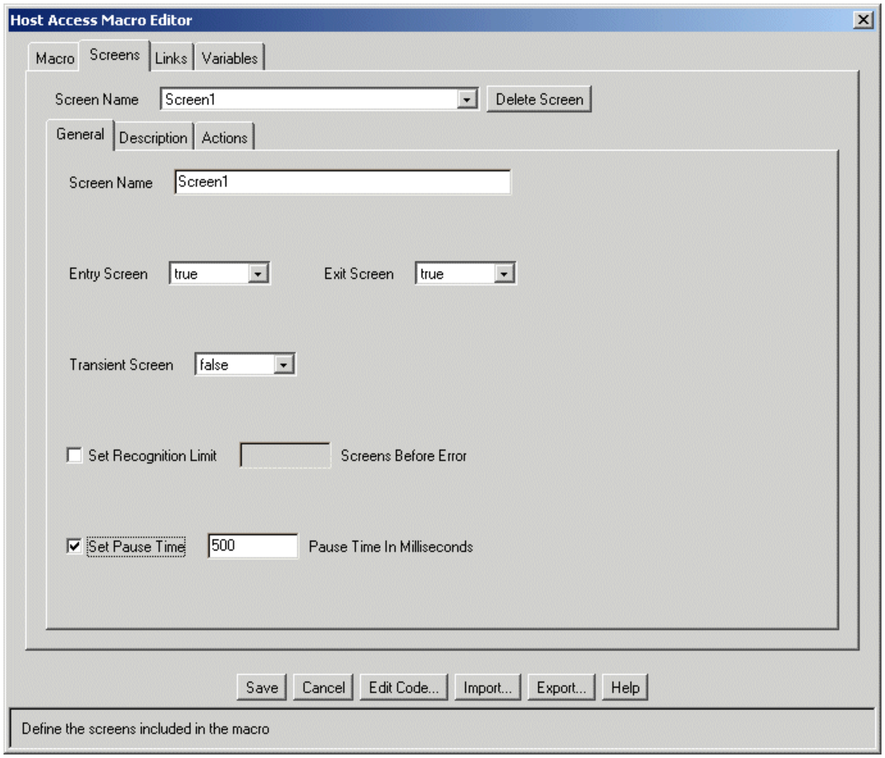
☑ Timeout Between Screens 60000 milliseconds

☑ Show All Prompts at Start of Macro

☑ Use Variables and Arithmetic Expressions In Macro

Define the general attributes of the macro

Figure 22-17 Global screen timeouts



Screen Name: Screen1

Screen Name: Screen1

Entry Screen: true

Exit Screen: true

Transient Screen: false

☐ Set Recognition Limit Screens Before Error

☑ Set Pause Time 500 Pause Time In Milliseconds

Define the screens included in the macro

Figure 22-18 Screen unique pause time

22.5.5 Use of inverse Descriptor

When the option to use inverse descriptor for a screen is set, this tells the Macro processing to recognize a screen where the event does *not* appear. This can be useful when defining a screen, and you are not sure what will appear on a screen, but certainly know what will not appear.

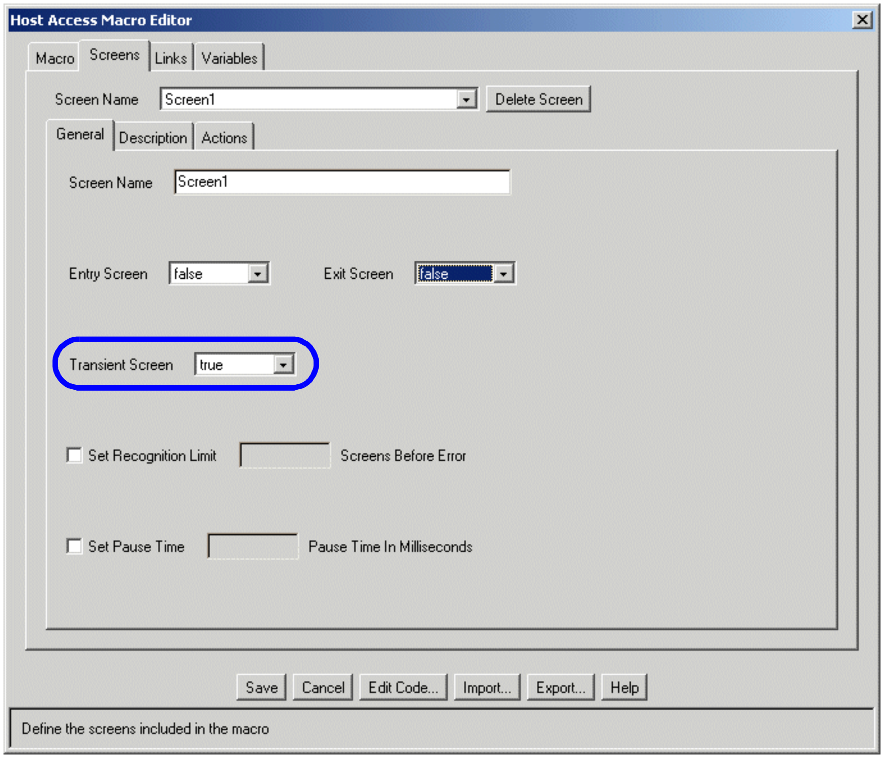
Table 22-1 Inverse descriptors

Descriptor	Inverse descriptor means
Cursor	If you select true, the cursor defined by this descriptor must not be at the specified cursor Row and Column.
Attribute	If you select true, the attribute defined by this descriptor must not appear on the session screen at the specific coordinate specified

Descriptor	Inverse descriptor means
String	If you select true, the string defined by this descriptor must not appear in the area defined by Start Row, Start Column, End Row, and End Column.
Field Counts	If Optional is true for Number of Fields, the number of fields on the screen should not equal the descriptor value. If Optional is true for Number of Input fields, the number of input fields on the screen should not equal the descriptor value.

22.5.6 Unexpected screens from the host

It is imperative that you define all possible screens the host may send during the time that a Macro executes. If you fail to do this, then the Macro logic will timeout when a new screen shows up that is unexpected while it waits for the expected screen. If the order of screens being presented may change, then you must change the screen logic appropriately.



Screen Name Screen1

Screen Name Screen1

Entry Screen false

Exit Screen false

Transient Screen true

□ Set Recognition Limit Screens Before Error

□ Set Pause Time Pause Time In Milliseconds

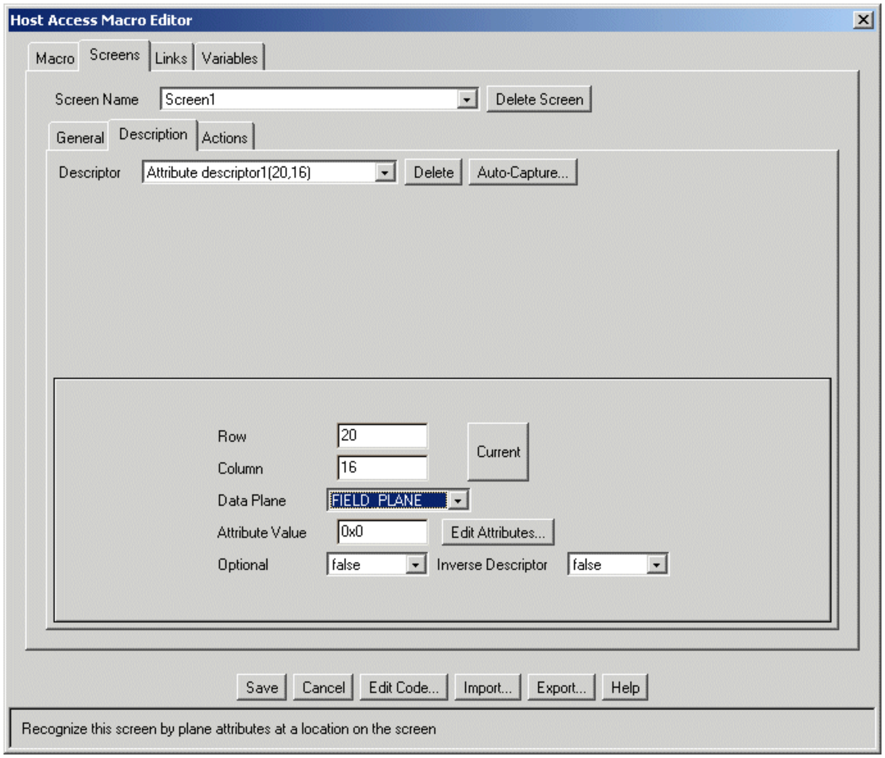
Define the screens included in the macro

Figure 22-19 Setting Up Transient Screen after Capture

For situations involving a screen that may randomly occur anytime during the Macro execution, you may want to consider capturing this screen as a transient screen. The Macro will check for transient screens on every new host screen update. This can be useful for screens, such as operator messages or system warnings. Use the Macro Manager to capture this transient screen and add it into the Macro logic flows.

Note: Be sure to set the option Transient Screen to `True`. See Figure 22-19.

22.5.7 Screen attributes



Screen Name: Screen1

Descriptor: Attribute descriptor1(20,16)

Row: 20

Column: 16

Data Plane: FIELD_PLANE

Attribute Value: 0x0

Optional: false

Inverse Descriptor: false

Recognize this screen by plane attributes at a location on the screen

Figure 22-20 Using Attribute Descriptor

You can add additional screen descriptors to your screen to insure recognition of the correct screen. The attribute descriptor allows you to recognize a screen by plane attributes (color, field, or extended field) at a specified row and column position. See Figure 22-20.

22.5.8 Screen scroll problems - adding looping to Macro

If you have a host screen that contains a list that you scroll through, you may face a situation where the list gets added to, and flows onto an additional host page that your Macro logic is not prepared for. To handle this you can add looping into the Macro logic.

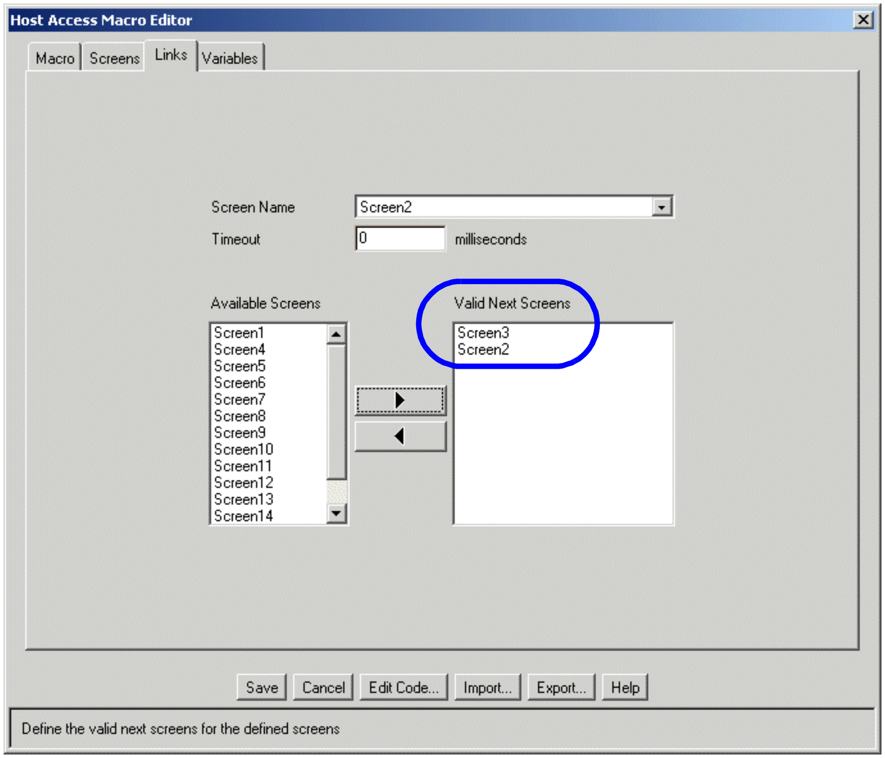
Assume the logic in your Macro is something simple like:

- Recognize the first screen in the list, call this screen 1.
- Press **F6** to scroll to next page, call this screen 2.
- Press F6 to scroll to next page, call this screen 3.

- Read the value for an entry from screen 3.

At a later time, someone added some new items in front of your selected item in the list. Now the logic would require you to press F6 an additional time. There is now a screen after step 3 above that you must scroll to. You can prepare for this if you use the Macro manager and add the following to screen 2:

- Modify the screen description for screen 2 by adding the Valid Next screen for screen 2 to include screen 2. See Figure 22-21.



Screen Name: Screen2

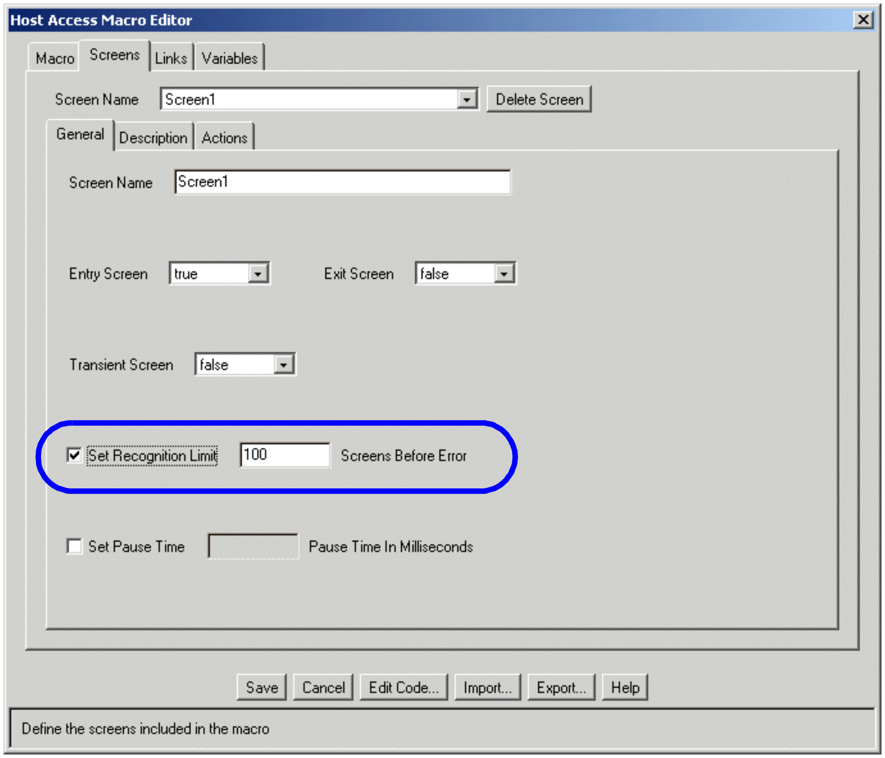
Timeout: 0 milliseconds

Valid Next Screens: Screen3, Screen2

Define the valid next screens for the defined screens

Figure 22-21 Screen links to allow looping

- Add the Inversion String Descriptor (see 22.5.5, “Use of inverse Descriptor” on page 800) to Screen 2. This will have the effect of allowing screens to continue to execute itself as long as the field you are scrolling to locate does *not* exist on screen 2.
- Set the Screen Recognition Limit to prevent looping forever. See Figure 22-22.



Screen Name: Screen1

Screen Name: Screen1

Entry Screen: true

Exit Screen: false

Transient Screen: false

☑ Set Recognition Limit 100 Screens Before Error

☐ Set Pause Time Pause Time In Milliseconds

Define the screens included in the macro

Figure 22-22 Setting screen recognition limit

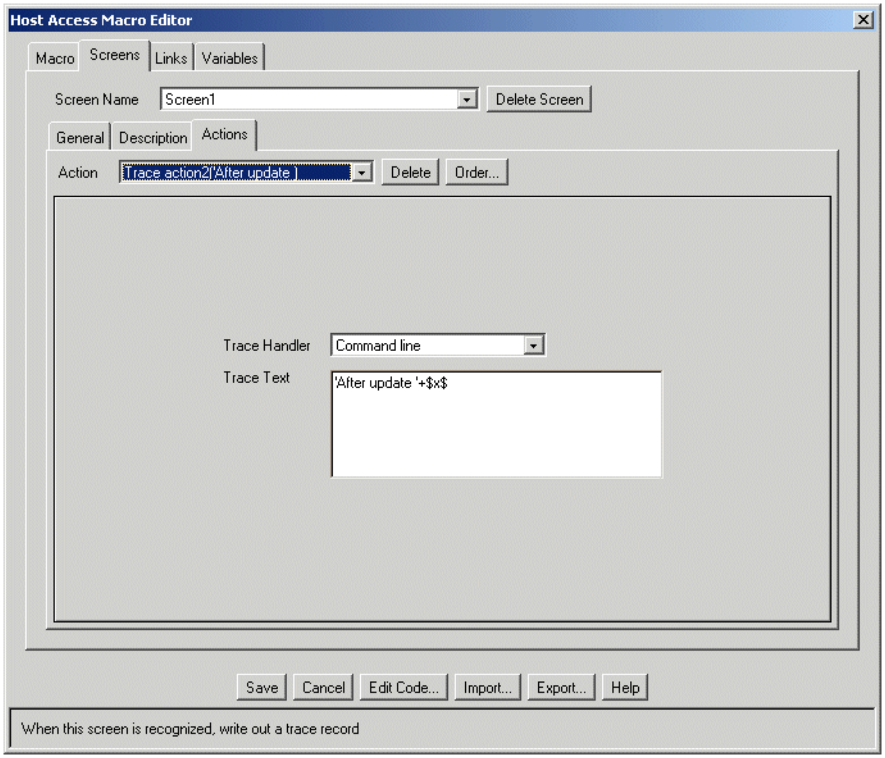
When you finally exit from screen 2, it will go to screen 3 where you can read the value you have been scrolling to locate.

22.6 Problem determination tools and strategies

In the following section are some means of problem determination and solving.

22.6.1 Adding trace statements to Macros

Macros are easily debugged using the ability to direct trace output to the Java console. Use the Macro Manager to add the Action trace action() to your Macro. Be sure you use the order option to place the trace option in the appropriate location in the sequence of actions that occur for the screen.



Screen Name: Screen1

Action: Trace action2('After update)

Trace Handler: Command line

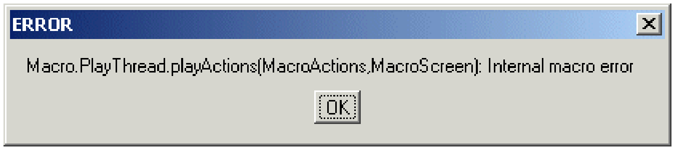
Trace Text: 'After update '+x

When this screen is recognized, write out a trace record

Figure 22-23 Adding trace for Variable X in a Macro

22.6.2 Errors with HOD Macro variables

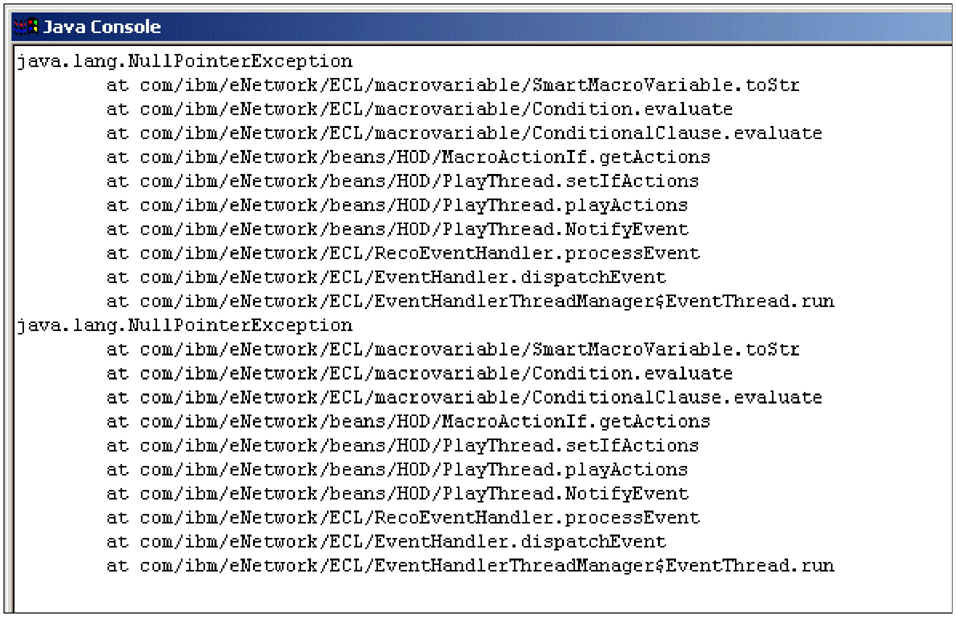
When your HOD Macro becomes large and complicated enough you will undoubtedly have a few programming errors. For instance, if you attempt to use a variable before it is defined you may see this error displayed in the browser when the Macro executes as shown in Figure 22-24.



Macro.PlayThread.playActions(MacroActions,MacroScreen): Internal macro error

Figure 22-24 Undefined variable error

The Java console in the meantime will trace some additional errors as seen in Figure 22-25.

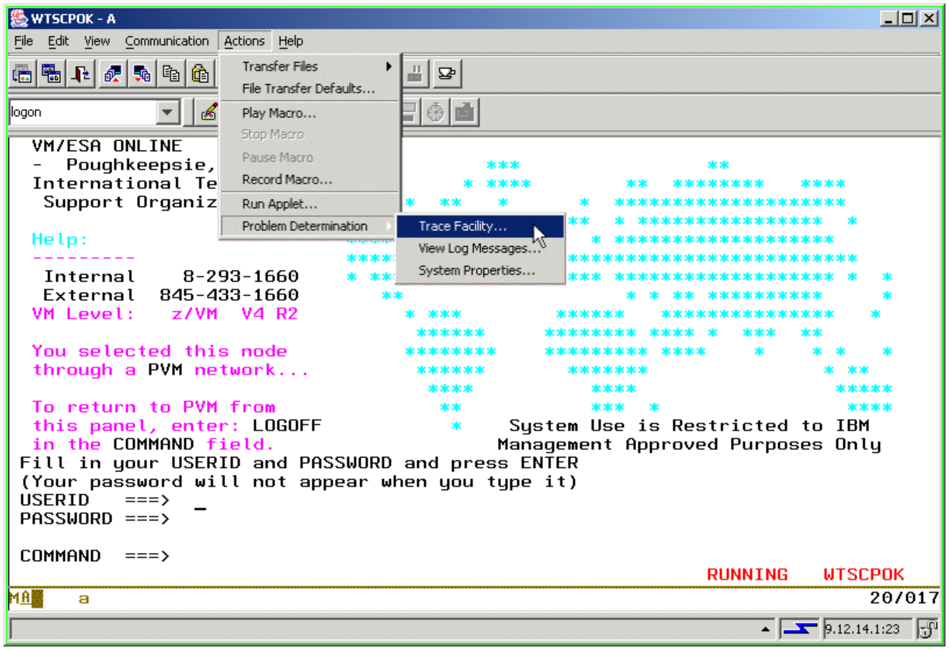


```
java.lang.NullPointerException
        at com/ibm/eNetwork/ECL/macrovariable/SmartMacroVariable.toStr
        at com/ibm/eNetwork/ECL/macrovariable/Condition.evaluate
        at com/ibm/eNetwork/ECL/macrovariable/ConditionalClause.evaluate
        at com/ibm/eNetwork/beans/HOD/MacroActionIf.getActions
        at com/ibm/eNetwork/beans/HOD/PlayThread.setIfActions
        at com/ibm/eNetwork/beans/HOD/PlayThread.playActions
        at com/ibm/eNetwork/beans/HOD/PlayThread.NotifyEvent
        at com/ibm/eNetwork/ECL/RecoEventHandler.processEvent
        at com/ibm/eNetwork/ECL/EventHandler.dispatchEvent
        at com/ibm/eNetwork/ECL/EventHandlerThreadManager$EventThread.run
java.lang.NullPointerException
        at com/ibm/eNetwork/ECL/macrovariable/SmartMacroVariable.toStr
        at com/ibm/eNetwork/ECL/macrovariable/Condition.evaluate
        at com/ibm/eNetwork/ECL/macrovariable/ConditionalClause.evaluate
        at com/ibm/eNetwork/beans/HOD/MacroActionIf.getActions
        at com/ibm/eNetwork/beans/HOD/PlayThread.setIfActions
        at com/ibm/eNetwork/beans/HOD/PlayThread.playActions
        at com/ibm/eNetwork/beans/HOD/PlayThread.NotifyEvent
        at com/ibm/eNetwork/ECL/RecoEventHandler.processEvent
        at com/ibm/eNetwork/ECL/EventHandler.dispatchEvent
        at com/ibm/eNetwork/ECL/EventHandlerThreadManager$EventThread.run
```

Figure 22-25 Java Console when Macro Error occurs

22.6.3 Using problem determination trace

The most powerful debug tool available when trying to determine why a Macro is not working is the problem determination trace. This facility is available when you are using HOD Clients with Problem Determination.

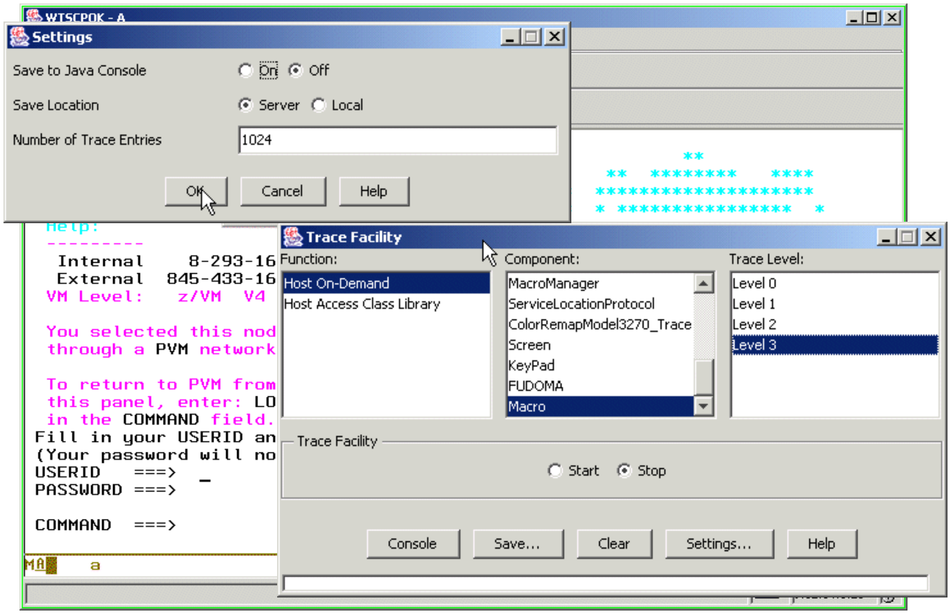


```
 VM/ESA ONLINE
 -  Poughkeepsie,
 International Te
  Support Organiz

 Help:
 ---------
  Internal    8-293-1660
  External  845-433-1660
 VM Level:   z/VM  V4 R2

 You selected this node
 through a PVM network...

 To return to PVM from
 this panel, enter: LOGOFF                   System Use is Restricted to IBM
 in the COMMAND field.                      Management Approved Purposes Only
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>  _
PASSWORD ===>

COMMAND  ===>
                                                          RUNNING    WTSCPOK
MA     a                                                                20/017
```

Figure 22-26 Start problem determination trace

To start the Trace facility select from the Emulator Toolbar **Actions->Problem Determination Trace Facility**. See Figure 22-26.

Now you must turn on the appropriate problem determination trace, see Figure 22-27.



Save to Java Console ○ On ● Off

Save Location ● Server ○ Local

Number of Trace Entries 1024

Function: Host On-Demand (selected), Host Access Class Library

Component: MacroManager, ServiceLocationProtocol, ColorRemapModel3270_Trace, Screen, KeyPad, FUDOMA, Macro (selected)

Trace Level: Level 0, Level 1, Level 2, Level 3 (selected)

Trace Facility ○ Start ● Stop

Figure 22-27 Enabling Macro trace

Start the trace and then execute your Macro. Stop the trace and save the trace file. An example of trace output is shown in Example 22-4. This example illustrates the errors that are traced when the initial screen is not recognized.

Example 22-4 Macro problem determination trace

```
4@0@09/20/2002 08:52:16:580@Host On-Demand@Macro@?@setProperty():2: macroName=
4@1@09/20/2002 08:52:16:580@Host On-Demand@Macro@?@setProperty():2: macroDescription=
4@2@09/20/2002 08:52:16:580@Host On-Demand@Macro@?@setProperty():2: empty=true
4@3@09/20/2002 08:52:16:580@Host On-Demand@Macro@?@setProperty():2: state=6
4@4@09/20/2002 08:52:16:590@Host On-Demand@Macro@?@setProperty():2: macroName=logon
4@5@09/20/2002 08:52:16:590@Host On-Demand@Macro@?@setProperty():2: macroDescription=test
4@6@09/20/2002 08:52:16:590@Host On-Demand@Macro@?@setMacro input:
4@7@09/20/2002 08:52:16:590@Host On-Demand@Macro@?@<HAScript name="logon" description="test"
timeout="60000" pausetime="300" promptall="true" author="" creationdate=""
supressclearevents="false" usevars="false" >       <screen name="Screen1" entryscreen="true"
exitscreen="false" transient="false">          <description>            <oia
status="NOTINHIBITED" optional="false" invertmatch="false" />          </description>
<actions>            <input value="arc[tab]hod4mea[enter]" row="0" col="0" movecursor="true"
xlatehostkeys="true" encrypted="false" />         </actions>         <nextscreens timeout="0"
>             <nextscreen name="Screen2" />          </nextscreens>      </screen>
<screen name="Screen2" entryscreen="false" exitscreen="true" transient="false">
<description>        <oia status="NOTINHIBITED" optional="false" invertmatch="false" />
```

```
<numfields number="7" optional="false" invertmatch="false" />              <numinputfields
number="1" optional="false" invertmatch="false" />       </description>       <actions>
<input value="f[enter]" row="0" col="0" movecursor="true" xlatehostkeys="true"
encrypted="false" />          </actions>          <nextscreens timeout="0" >
</nextscreens>      </screen>    </HAScript>
4@8@09/20/2002 08:52:16:620@Host On-Demand@Macro@?@setProperty():2: empty=false
4@9@09/20/2002 08:52:16:620@Host On-Demand@Macro@?@setProperty():2: state=1
4@10@09/20/2002 08:52:16:620@Host On-Demand@Macro@?@setProperty():2: state=2
4@11@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@
4@12@09/20/2002 08:52:16:630@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@13@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@Macro debug starting.
4@14@09/20/2002 08:52:16:630@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@15@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@Warning, the screen could have been updated
between the screen
4@16@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@comparison and the trace log addition. For
this reason, the actual
4@17@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@contents of this trace will be slightly out
of sync and could
4@18@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@indicate a PASS or a FAIL when the opposite
is shown in the trace.
4@19@09/20/2002 08:52:16:630@Host On-Demand@Macro@?@This occurs particulary often with strings.
4@20@09/20/2002 08:52:16:630@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@21@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@
4@22@09/20/2002 08:52:16:650@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@23@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@Screen1, matched = true
4@24@09/20/2002 08:52:16:650@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@25@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@Macro action executing:
4@26@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@  Screen Name = Screen1
4@27@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@  Action Index = 0
4@28@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@  Action Info = <input
value="arc[tab]hod4mea[enter]" />
4@29@09/20/2002 08:52:16:650@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@30@09/20/2002 08:52:16:650@Host On-Demand@Macro@?@
4@31@09/20/2002 08:52:16:991@Host On-Demand@Macro@?@
4@32@09/20/2002 08:52:16:991@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@33@09/20/2002 08:52:16:991@Host On-Demand@Macro@?@Screen2, matched = false
4@34@09/20/2002 08:52:17:001@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@35@09/20/2002 08:52:17:001@Host On-Demand@Macro@?@  Screen Descriptor Details:
4@36@09/20/2002 08:52:17:001@Host On-Demand@Macro@?@    FAIL: <oia status="NOTINHIBITED" />
4@37@09/20/2002 08:52:17:001@Host On-Demand@Macro@?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
```

```
4@38@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <numfields number="7" />
4@39@09/20/2002 08:52:17:001@Host On-Demand@Macro?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@40@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <numinputfields number="1" />
4@41@09/20/2002 08:52:17:001@Host On-Demand@Macro?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@42@09/20/2002 08:52:17:001@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@43@09/20/2002 08:52:17:001@Host On-Demand@Macro?@
4@44@09/20/2002 08:52:17:001@Host On-Demand@Macro?@
4@45@09/20/2002 08:52:17:001@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@46@09/20/2002 08:52:17:001@Host On-Demand@Macro?@Screen2, matched = false
4@47@09/20/2002 08:52:17:001@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@48@09/20/2002 08:52:17:001@Host On-Demand@Macro?@  Screen Descriptor Details:
4@49@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <oia status="NOTINHIBITED" />
4@50@09/20/2002 08:52:17:001@Host On-Demand@Macro?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
4@51@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <numfields number="7" />
4@52@09/20/2002 08:52:17:001@Host On-Demand@Macro?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@53@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <numinputfields number="1" />
4@54@09/20/2002 08:52:17:001@Host On-Demand@Macro?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@55@09/20/2002 08:52:17:001@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@56@09/20/2002 08:52:17:001@Host On-Demand@Macro?@
4@57@09/20/2002 08:52:17:001@Host On-Demand@Macro?@
4@58@09/20/2002 08:52:17:001@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@59@09/20/2002 08:52:17:001@Host On-Demand@Macro?@Screen2, matched = false
4@60@09/20/2002 08:52:17:001@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@61@09/20/2002 08:52:17:001@Host On-Demand@Macro?@  Screen Descriptor Details:
4@62@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <oia status="NOTINHIBITED" />
4@63@09/20/2002 08:52:17:001@Host On-Demand@Macro?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
4@64@09/20/2002 08:52:17:001@Host On-Demand@Macro?@    FAIL: <numfields number="7" />
4@65@09/20/2002 08:52:17:011@Host On-Demand@Macro?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@66@09/20/2002 08:52:17:011@Host On-Demand@Macro?@    FAIL: <numinputfields number="1" />
4@67@09/20/2002 08:52:17:011@Host On-Demand@Macro?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@68@09/20/2002 08:52:17:011@Host
On-Demand@Macro?@------------------------------------------------------------------------
4@69@09/20/2002 08:52:17:011@Host On-Demand@Macro?@
4@70@09/20/2002 08:52:17:011@Host On-Demand@Macro?@
```

```
4@71@09/20/2002 08:52:17:011@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@72@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@Screen2, matched = false
4@73@09/20/2002 08:52:17:011@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@74@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@  Screen Descriptor Details:
4@75@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@    FAIL: <oia status="NOTINHIBITED" />
4@76@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
4@77@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@    FAIL: <numfields number="7" />
4@78@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@79@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@    FAIL: <numinputfields number="1" />
4@80@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@81@09/20/2002 08:52:17:011@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@82@09/20/2002 08:52:17:011@Host On-Demand@Macro@?@
4@83@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@
4@84@09/20/2002 08:52:17:081@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@85@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@Screen2, matched = false
4@86@09/20/2002 08:52:17:081@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@87@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@  Screen Descriptor Details:
4@88@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@    FAIL: <oia status="NOTINHIBITED" />
4@89@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
4@90@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@    FAIL: <numfields number="7" />
4@91@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@92@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@    FAIL: <numinputfields number="1" />
4@93@09/20/2002 08:52:17:081@Host On-Demand@Macro@?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@94@09/20/2002 08:52:17:081@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@95@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@
4@96@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@
4@97@09/20/2002 08:52:17:091@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@98@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@Screen2, matched = false
4@99@09/20/2002 08:52:17:091@Host
On-Demand@Macro@?@-------------------------------------------------------------------------
4@100@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@  Screen Descriptor Details:
4@101@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@    FAIL: <oia status="NOTINHIBITED" />
4@102@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
4@103@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@    FAIL: <numfields number="7" />
```

```
4@104@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@105@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@    FAIL: <numinputfields number="1" />
4@106@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@107@09/20/2002 08:52:17:091@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@108@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@
4@109@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@
4@110@09/20/2002 08:52:17:091@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@111@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@Screen2, matched = false
4@112@09/20/2002 08:52:17:091@Host
On-Demand@Macro@?@----------------------------------------------------------------------
4@113@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@  Screen Descriptor Details:
4@114@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@    FAIL: <oia status="NOTINHIBITED" />
4@115@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@      ACTUAL: <oia status="NOTINHIBITED"
optional="false" invertmatch="false" />
4@116@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@    FAIL: <numfields number="7" />
4@117@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@      ACTUAL: <numfields number="1"
optional="false" invertmatch="false" />
4@118@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@    FAIL: <numinputfields number="1" />
4@119@09/20/2002 08:52:17:091@Host On-Demand@Macro@?@      ACTUAL: <numinputfields number="1"
optional="false" invertmatch="false" />
4@120@09/20/2002 08:52:17:091@Host O
1@69@09/20/2002 08:52:33:164@pdpsi@?@?@line.separator =
1@70@09/20/2002 08:52:33:164@pdpsi@?@?@java.vm.name = Java HotSpot(TM) Client VM
1@71@09/20/2002 08:52:33:164@pdpsi@?@?@user.region = US
1@72@09/20/2002 08:52:33:164@pdpsi@?@?@file.encoding = Cp1252
1@73@09/20/2002 08:52:33:164@pdpsi@?@?@acl.write.default =
1@74@09/20/2002 08:52:33:164@pdpsi@?@?@browser.vendor = Sun Microsystems, Inc.
1@75@09/20/2002 08:52:33:164@pdpsi@?@?@java.specification.version = 1.3
```

23

Sharing and reusing objects

This chapter describes two new features introduced in Host On-Demand V8:

- Sharing and reusing of objects (macros, keyboard and toolbar components)
- Server macro library support

23.1 Overview

Host On-Demand sessions can now use macros, keyboard, and toolbar definitions that are external to the session configuration. Prior to Host On-Demand Version 8, the definitions for these components needed to be part of the session itself. Although you can store macros as files, you still had to import them into the session before you can use them. This new capability of the session to use external definitions greatly simplifies the task of sharing and reusing these important components. Host on Demand V8 still can use the macros, keyboard, and toolbar definitions as imbedded data from Host on Demand V7. The new function of sharing this data was added to Host on Demand V8 without removing the old capability.

23.1.1 Sharing and reusing objects

Sharing and reusing macros, and keyboard and toolbar definition files is available to administrators who can use these objects and configure them into the sessions, ready for use by the clients. Users as well can create their own objects and use them across their sessions at the client machine.

The following files can be shared:

- *.mac = macro file
- *.kmp = keyboard map file
- *.bar = toolbar definition file

Even though the file names suggest their format is common with those of Personal Communications, these files are not interchangeable with Personal Communications.

The component macros, keyboard maps, and toolbar remaps may reside on the following locations:

- Current session - Subcomponent is imbedded within the session configuration (toolbar, keyboard or macro)
- File (keyboard and toolbar) - Subcomponent is separately stored as a *.kmp or *.bar file
- Personal Library - Read and write disk space of user and path ending with HODObjs
- Server Library - Macro Library created by administrator on a shared network drive or in the Web (read only for users)

23.1.2 Server macro libraries

Server macro libraries are available for the HTML model session only. They allow you to create and maintain a central repository of macros for users to access from their Host On-Demand sessions. These macros are not downloaded to the user's machine until they are needed. When you make changes to a server macro, users automatically get your updates the next time they access the macro.

Server macro libraries have several benefits:

- They provide a convenient way to store, edit, and administer macros, all from one easy-to-access location.
- They allow easy sharing of macros among multiple users and across any number of sessions.
- They eliminate the need to import macros into the Host On-Demand session, and can therefore reduce the size of the session. The macros are only downloaded to the user's machine if and when the user accesses them.
- You can edit macros and replace the files in the server macro library at any time without regenerating Host On-Demand sessions or modifying the HTML files. Any changes you make are automatically available the next time a user requests that macro.
- Sessions can be configured so they can access only a subset of the macros out of the server library macro pool (using the macro list file).

Server macro libraries are read-only for users and can reside on a Web server or on a shared network drive. For both types of libraries, you can control which macros are available to particular Host On-Demand sessions. If you use a Web-based macro library, you need to create a text file that identifies the specific macros that you want to be available for the session that you are configuring. If you use a shared drive-based macro library, then all the files in the specified directory will be available to the session. You can use different directories with different sets of macros for different sessions. Which type of server macro library you choose depends on your computing environment as well as your company needs.

23.2 Planning

Because users and administrators have different goals when planning for these functions, we have split this section into a discussion for users and a discussion for administrators.

23.2.1 Users

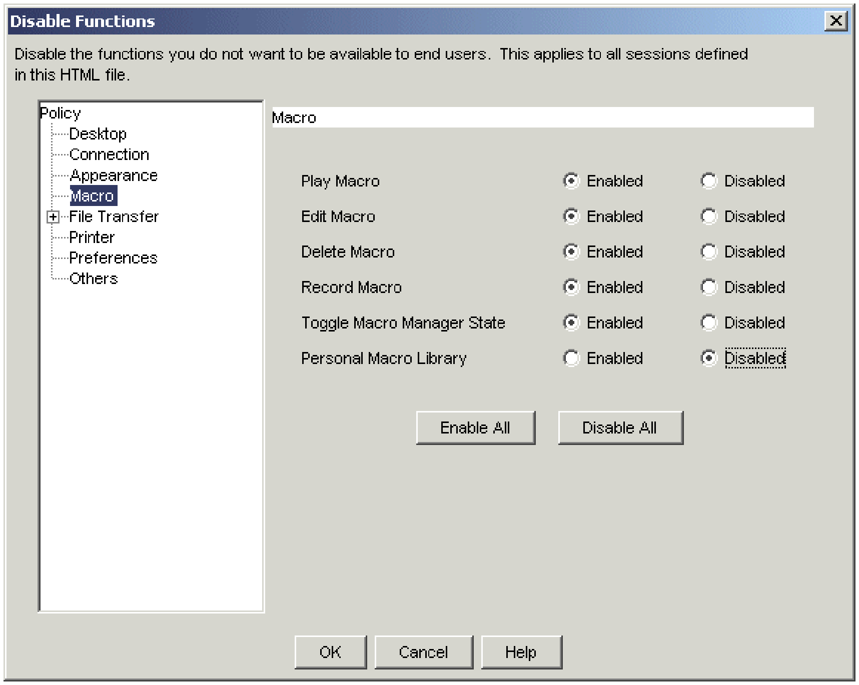
Users can define macro, keyboard, or toolbar definitions and save them into separate files (Personal Library). These separate files are then immediately available to other sessions. You no longer need to configure the identical component again for the new session or to import the macro file. If the user subsequently updates any of these macro, keyboard, or toolbar definition files, other sessions that use those external files from the personal library will automatically get the updates.

By default, the macro, keyboard, and toolbar component files that users create are stored on their local machines in the HODObjs subdirectory. The complete path for the HODObjs subdirectory is a writable location unique to the user, and the exact path depends on the platform, browser, and JVM level. A typical path on a Windows machine using IE, for example, might be:

```
Documents and Settings\username\HODObjs\
```

If the administrator has configured an alternate save location (using the save HTML parameter), then that location will be used for storing the component files.

The administrator can prevent users from creating and using their own macros in a personal macro library by disabling that function in the **Disable** function as shown in the example of Deployment Wizard configuration in Figure 23-1.



Disable Functions

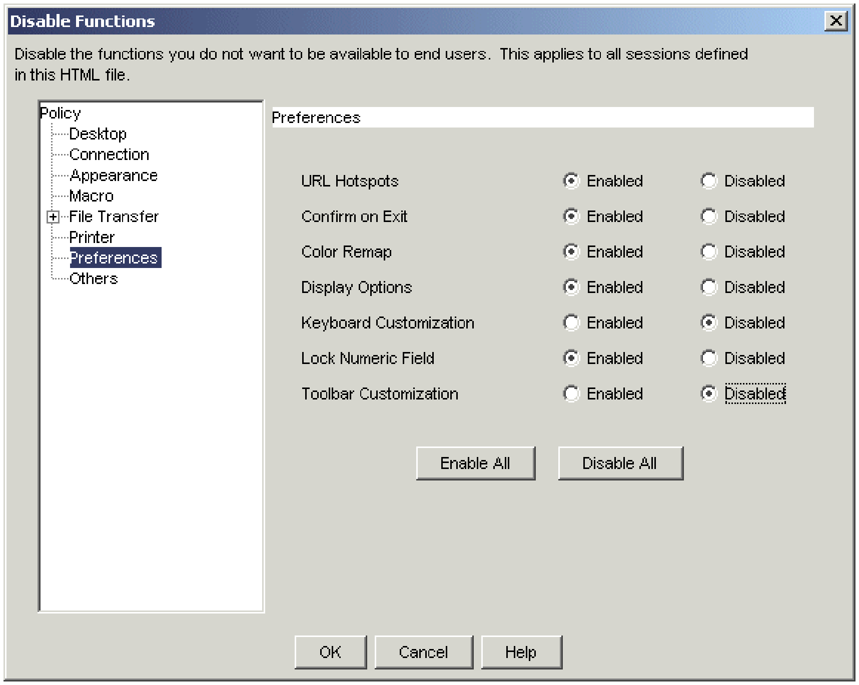
Disable the functions you do not want to be available to end users. This applies to all sessions defined in this HTML file.

Macro

Play Macro	● Enabled	○ Disabled
Edit Macro	● Enabled	○ Disabled
Delete Macro	● Enabled	○ Disabled
Record Macro	● Enabled	○ Disabled
Toggle Macro Manager State	● Enabled	○ Disabled
Personal Macro Library	○ Enabled	● Disabled

Figure 23-1   Disabling usage of Personal Macro Library

The administrator can prevent users from creating and using their own toolbars by disabling those functions in the **Disable** function as shown in the example of Deployment Wizard configuration in Figure 23-2.



Disable the functions you do not want to be available to end users. This applies to all sessions defined in this HTML file.

URL Hotspots	● Enabled	○ Disabled
Confirm on Exit	● Enabled	○ Disabled
Color Remap	● Enabled	○ Disabled
Display Options	● Enabled	○ Disabled
Keyboard Customization	○ Enabled	● Disabled
Lock Numeric Field	● Enabled	○ Disabled
Toolbar Customization	○ Enabled	● Disabled

Figure 23-2 Disabling toolbar and keyboard configuration

23.2.2 Administrators

The fact that macros, keyboard, and toolbar definitions can exist as separate files makes it easier for you to reuse components when you are configuring sessions for your users. However, you should understand that these sessions should not normally point to file components, since the files are not distributed to your users along with the session definitions. Generally, any macro, keyboard, or toolbar definition that you want to make available to your users should be saved in the Current Session.

You can configure sessions from either the Deployment Wizard (for the HTML model) or the Host On-Demand Administration Utility (for the Configuration server-based and Combined models). In either case, you can start the sessions you wish to configure, and from the launched sessions, you will have access to all the user functions relating to macro, keyboard, and toolbar definitions that are discussed above. Copy and save the objects in the session so that those get downloaded to the user along with the session.

An exception to that rule is server macro libraries where the macros reside on a Web or network shared resource. The session definition contains only a pointer to those. In that case no component (= no macro) will be downloaded to user.

23.3 Installation and configuration

Because users and administrators have different goals when installing and configuring these functions, we have split this section into a discussion for users and a discussion for administrators.

23.3.1 Users

Macros

All of the session dialogs that list available macros, such as the Play Macro window, allow you to select a macro location. Possible locations include the following:

- Current Session, which lists the macros embedded in the session
- Personal Library, which lists the macros in the HODObjs subdirectory
- Server Library, which lists the macros in the server macro library, if one has been configured by the administrator

When users record new macros or update existing ones, they have the option to save them to either the Current Session or to their new Personal Library. Also, on the Available Macros window, which is available from the drop-down menu on the Macro Manager toolbar, users can copy and paste any number of macros from one macro location to another.

We used some of these functions in 23.5, “Scenario using server macro libraries” on page 834. Please refer to that section for some examples.

The following functions are also available when you right-click a macro file name in the macro list window:

- Copy
- Paste
- Cut
- Delete
- Properties

You cannot paste, cut, or delete macros when working with the server macro library location because it is read-only for users.

Copy

To copy a macro, select a macro or a set of macros in the list, right-click the file names, and select **Copy**. This copies the macros into the Macro clipboard from which you can paste into a different location.

Paste

Paste copies the macros that are in the Macro clipboard (as a result of a previous Cut or Copy operation) to the specified location.

Pasting a macro to a new location can have some unexpected results with regard to how it is named. Macros listed in the current session are identified by the macro name itself, whereas macros in personal or server libraries are identified by their file names.

Note the following:

- If a macro from the current session is pasted to the personal library, the new file name is the macro name with a .mac extension appended to it.
- If a macro from the personal or server libraries is pasted to the current session, the macro is listed as its macro name.
- If a macro from the server library is pasted to the personal library, the new file is given the old file name.

Cut

To cut a macro, select a macro or a set of macros in the list, right-click the file names, and select **Cut**. The macro or set of macros continue to reside in the Available macros list as well as in the Macro clipboard until you paste it into another location.

Delete

To delete a macro, select a macro or a set of macros in the list, right-click the file name, and select **Delete**. You cannot use the Available macros window to delete the current macro that is displayed in the Macro Manager. To delete the current macro, you must use the Macro Manager's **Delete** button.

Properties

To view a macro's properties, select a macro in the list of available macros, right-click the file name, and select **Properties**. A window appears that lists the macro name, description, author, creation date, and macro location. You cannot edit macro properties from this window. To edit macro properties, you must use the Macro Editor.

Keyboard

The **Open** button on the keyboard window allows users to change the current keyboard definition being used by the session. At any given time, there is only one keyboard definition associated with an active session, but users can open a different one whenever the need arises. The **Open** button launches a window that allows users to choose either the legacy keyboard defined internally in the session (the **Current Session** option) or an external file. Users can open a keyboard definition file from any location on their system, but the default location is the HODObjs subdirectory. Regardless of which keyboard definition the user opens, the selected definition becomes the current one used by the Host On-Demand session. Any updates that the user makes to the keyboard using the **Save** button are saved back to the location from which the keyboard was loaded (either the current session or the particular file). The next time the user launches the session, the same keyboard is automatically loaded from either the current session or the file.

The **Save As** button on the keyboard window allows users to save the current keyboard definition to a different location or file than is currently being used by the session. When the user selects **Save As**, the newly-saved keyboard becomes the current one for the session. This means that the saved keyboard will be the one loaded the next time the user launches the session.

Toolbar

Like the keyboard, the toolbar offers the **Open** and **Save As** options. These options are available by clicking **Edit ->Preferences ->Toolbar** in a host session or by right-clicking the toolbar itself.

23.3.2 Administrators

The following examples demonstrate the steps you need to follow to use the file components in a session that you are configuring for your users.

Macros

An administrator is configuring an HTML file in the Deployment Wizard (DW) and starts one of the sessions. After configuring three macros, he realizes these macros might be useful for other sessions as well. He copies the macros from the Current Session to his Personal Library, using the copy and paste feature of the Available Macros panel. Later, when configuring a different HTML file in the Deployment Wizard, he decides to use those same three macros for one of the new sessions. He starts the new session and copies the three macros from his Personal Library to the Current Session, again using the copy/paste feature.

Toolbar

An administrator is configuring a group session in the Host On-Demand Administration Utility. He wishes to incorporate a toolbar definition that one of his users sent to him in an e-mail. He saves the toolbar file onto his machine, and then starts the session that he wants to configure in the Host On-Demand Administration Utility. He right-clicks from toolbar **File**, and browses to the toolbar file on his local machine. When found, he selects it and clicks **OK**. At this point, the toolbar settings will change to the settings in the toolbar file. Next, he right-clicks the toolbar and selects **Save As**. He selects **Current Session** and then clicks **OK**. He must follow the **Save As** step to save the toolbar definition into the session and make it available to his users. If he does not follow the Save As step, then when the user starts the session, Host On-Demand will search for the file on the user's local machine, and it will not find it.

Keyboard

Refer to the Toolbar example above. Follow the same steps, except with the keyboard file.

Additional enhancements for the administrator

For an HTML model only:

- Host On-Demand offers an import (and export) capability for both keyboard and toolbar definitions in the Deployment Wizard. These functions are available from the Configure menu on the Host Sessions window, and give administrators an easier way to incorporate keyboard or toolbar component files into the session they are configuring for their users.
- When you import a keyboard or toolbar definition into the session definition (as described in the first enhancement above), Host On-Demand uses that definition any time users reset their current keyboard or toolbar to its default value. For example, if you import a keyboard definition into a session for your users, then any time that a user is editing keyboard settings, and selects **Reset All**, the current keyboard will be restored to the imported keyboard values. If you have not imported a keyboard or toolbar definition into the session, and user clicks **Reset All**, and the values become the default ones provided with Host On-Demand.
- You can now create and deploy server macro libraries and make the macros in these libraries available on the server for specified sessions. The individual macros from the library are only downloaded to the user's machine when and if the user requests them. You can control which macros are available to which sessions. You can also update the macros in the library at any time, and the changes will be available for users the next time they access the macro.

23.4 Scenario using sharing and reusing objects

Because users and administrators have different goals when creating and using these functions, we have split this section into a discussion for users and a discussion for administrators.

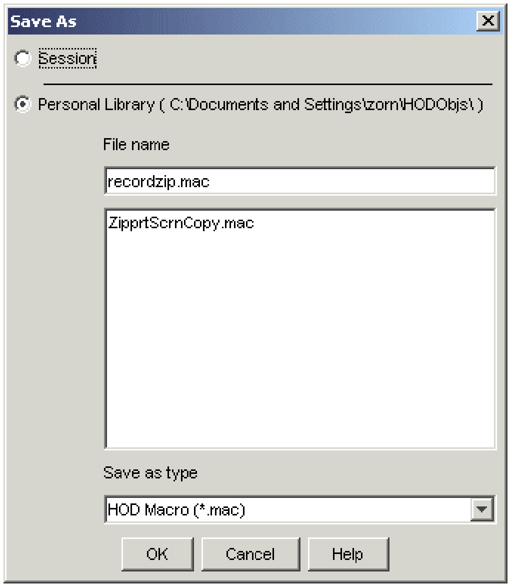
23.4.1 Users

Use shared objects only among similar sessions. For example, a toolbar from a 3270 session with send and receive files might cause problems at a 5250 session.

Macro

As a user we have written a little macro, which copies the text of a screen and prints it. We want to use it in another session too.

When saving it from the macro manager we clicked **Save as**. The window shown in Figure 23-3 appears.



○ Session

● Personal Library (C:\Documents and Settings\zorn\HODObjs\ )

File name: recordzip.mac

ZipprtScrnCopy.mac

Save as type: HOD Macro (*.mac)

Figure 23-3 User saves macro for sharing

We save the macro as a file recordzip.mac in the personal library HODObjs subdirectory. Now we can use it in another display session: We open the macro editor and click at its pull-down menu to open. It presents the window to select macros from within the current session or from the locally stored personal library.

We have chosen the personal library into which we had saved the macro from the first session (Figure 23-4).You will notice that this window does not show a server macro library. Reason for that is: At that time the administrator had not yet defined a server macro library.

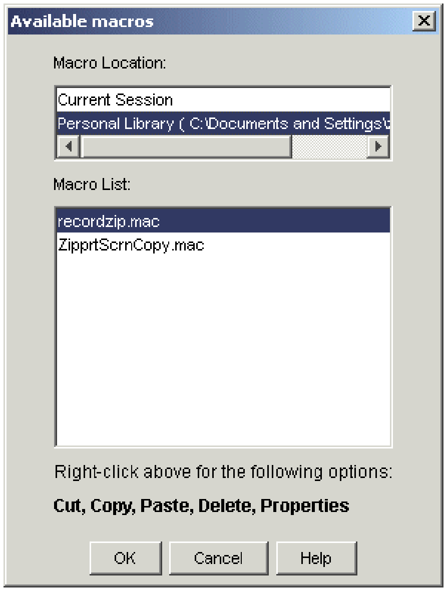
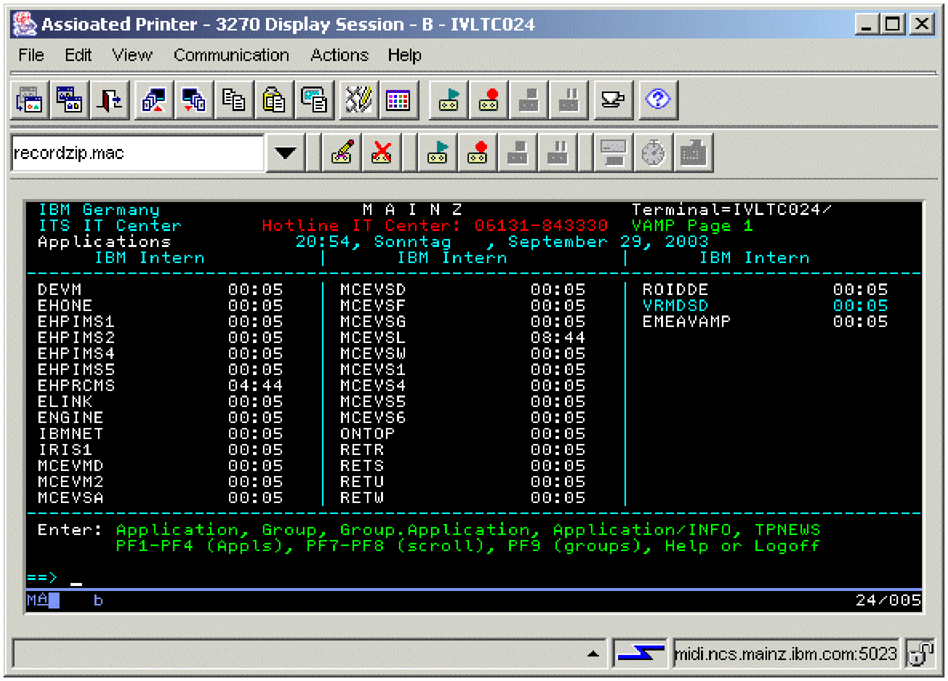

Available macros
Macro Location:
Current Session
Personal Library (C:\Documents and Settings\
Macro List:
recordzip.mac
ZipprtScrnCopy.mac
Right-click above for the following options:
Cut, Copy, Paste, Delete, Properties
OK
Cancel
Help

Figure 23-4 Available macros as shared at a user machine

From here we selected our macro recordzip.mac and clicked **OK**. As seen in Figure 23-5, it is now ready to be used in this second session. Using this process we have not imbedded the macro into our current session, we have selected it only to access it as an external shared object.


Assioated Printer - 3270 Display Session - B - IVLTC024
File Edit View Communication Actions Help
recordzip.mac
midi.ncs.mainz.ibm.com:5023

```
 IBM Germany                  M A I N Z                Terminal=IVLTC024/
 ITS IT Center          Hotline IT Center: 06131-843330  VAMP Page 1
 Applications              20:54, Sonntag    , September 29, 2003
      IBM Intern              |       IBM Intern         |       IBM Intern
-----------------------------------------------------------------------------
 DEVM              00:05      | MCEVSD            00:05  | ROIDDE            00:05
 EHONE             00:05      | MCEVSF            00:05  | VRMDSD            00:05
 EHPIMS1           00:05      | MCEVSG            00:05  | EMEAVAMP          00:05
 EHPIMS2           00:05      | MCEVSL            08:44  |
 EHPIMS4           00:05      | MCEVSW            00:05  |
 EHPIMS5           00:05      | MCEVS1            00:05  |
 EHPRCMS           04:44      | MCEVS4            00:05  |
 ELINK             00:05      | MCEVS5            00:05  |
 ENGINE            00:05      | MCEVS6            00:05  |
 IBMNET            00:05      | ONTOP             00:05  |
 IRIS1             00:05      | RETR              00:05  |
 MCEVMD            00:05      | RETS              00:05  |
 MCEVM2            00:05      | RETU              00:05  |
 MCEVSA            00:05      | RETW              00:05  |
-----------------------------------------------------------------------------
 Enter: Application, Group, Group.Application, Application/INFO, TPNEWS
        PF1-PF4 (Appls), PF7-PF8 (scroll), PF9 (groups), Help or Logoff

==> _
MA      b                                                              24/005
```

Figure 23-5   Shared macro selected

The following limitation and recommendations apply:

- User cannot save macros to the server library (read only for users).
- Shared macros can only be used in the Host on Demand environment. Beans and HACL can only access macros that are imbedded in the session.
- Shared macros located locally or at the server cannot be used as Auto-Start macro.
- Host on Demand lists only shared macros with the extension *.mac.
- The macro file name should always be the same as the macro name stored within that file.
- Chaining of macros is only allowed for macros within the same location.

  For chaining macros imbedded in session use the macro name:

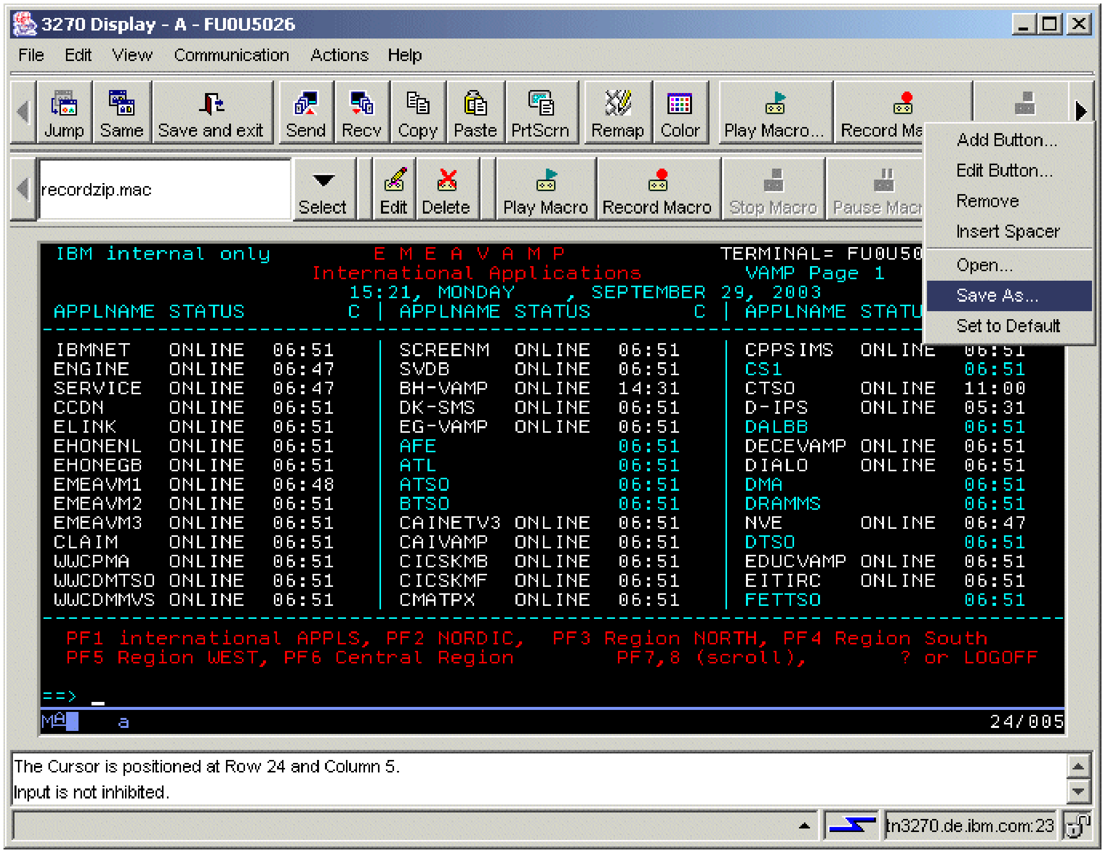
  ```
  <playmacro name=”nextMacro”.../>
  ```

For chaining macros from personal and server library use the macro file name with extension:

```
<playmacro name=”nextMacro.mac”.../>
```

Toolbar and keyboard

For saving the toolbar from the first session for sharing, place the mouse pointer over the toolbar and right-click.



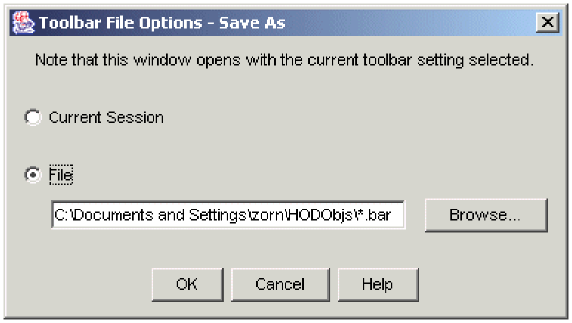
```
 IBM internal only          E M E A V A M P            TERMINAL= FU0U50
                      International Applications          VAMP Page 1
                         15:21, MONDAY     , SEPTEMBER 29, 2003
 APPLNAME STATUS            C | APPLNAME STATUS         C | APPLNAME STATU
 ----------------------------------------------------------------------------
 IBMNET   ONLINE  06:51       | SCREENM  ONLINE  06:51    | CPPSIMS  ONLINE  06:51
 ENGINE   ONLINE  06:47       | SVDB     ONLINE  06:51    | CS1              06:51
 SERVICE  ONLINE  06:47       | BH-VAMP  ONLINE  14:31    | CTSO     ONLINE  11:00
 CCDN     ONLINE  06:51       | DK-SMS   ONLINE  06:51    | D-IPS    ONLINE  05:31
 ELINK    ONLINE  06:51       | EG-VAMP  ONLINE  06:51    | DALBB            06:51
 EHONENL  ONLINE  06:51       | AFE              06:51    | DECEVAMP ONLINE  06:51
 EHONEGB  ONLINE  06:51       | ATL              06:51    | DIALO    ONLINE  06:51
 EMEAVM1  ONLINE  06:48       | ATSO             06:51    | DMA              06:51
 EMEAVM2  ONLINE  06:51       | BTSO             06:51    | DRAMMS           06:51
 EMEAVM3  ONLINE  06:51       | CAINETV3 ONLINE  06:51    | NVE      ONLINE  06:47
 CLAIM    ONLINE  06:51       | CAIVAMP  ONLINE  06:51    | DTSO             06:51
 WWCPMA   ONLINE  06:51       | CICSKMB  ONLINE  06:51    | EDUCVAMP ONLINE  06:51
 WWCDMTSO ONLINE  06:51       | CICSKMF  ONLINE  06:51    | EITIRC   ONLINE  06:51
 WWCDMMVS ONLINE  06:51       | CMATPX   ONLINE  06:51    | FETTSO           06:51
 ----------------------------------------------------------------------------
   PF1 international APPLS, PF2 NORDIC,  PF3 Region NORTH, PF4 Region South
   PF5 Region WEST, PF6 Central Region        PF7,8 (scroll),        ? or LOGOFF

==> _
MA       a                                                              24/005
```

```
The Cursor is positioned at Row 24 and Column 5.
Input is not inhibited.
```

tn3270.de.ibm.com:23

Figure 23-6 Toolbar submenu

The menu as shown in Figure 23-6 will appear from which we select **Save As...**



Toolbar File Options - Save As

Note that this window opens with the current toolbar setting selected.

○ Current Session

● File

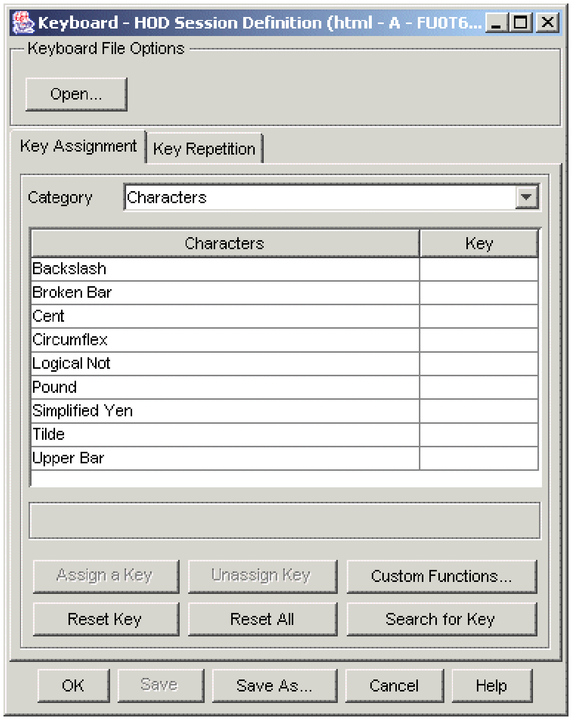
C:\Documents and Settings\zorn\HODObjs\*.bar

Figure 23-7 Toolbar File Save Options

Now we select radio button **File** to store the toolbar in a file. By default this option points to the HODObjs subdirectory for the user where we save the toolbar. In the session in which we want to use that toolbar, we use the menu as in Figure 23-6 and select **Open.** From there we select our saved toolbar file, which will become at that point our active toolbar.

Those steps can as well be performed by clicking at the session’s menu bar Edit - Preferences - Toolbar.

For the keyboard definition file the same procedure applies. Either use form the session's menu bar **Edit -> Preferences -> Keyboard** or use the **Remap** icon from the icon bar. The keyboard remap window as shown in Figure 23-8 appears. From that click **Save As** to store a definition in the file, and in the new session click **Open** to use it.



Category: Characters

Characters	Key
Backslash	
Broken Bar	
Cent	
Circumflex	
Logical Not	
Pound	
Simplified Yen	
Tilde	
Upper Bar	

Figure 23-8 Keyboard definition window

23.4.2 Administrators

Some items to remember as administrator: Separate files for re-usable objects are not distributed when the configuration files are sent to the users.

File locations:

- For administrators the default personal library location is HODObj directory.
- For the Deployment Wizard the HODOjs directory is in the install location of the Deployment Wizard.
- When running the Host on Demand administration client, the HODOBjs will be in Documents and Settings of the machine where the Host on Demand administration client is running.

Macro

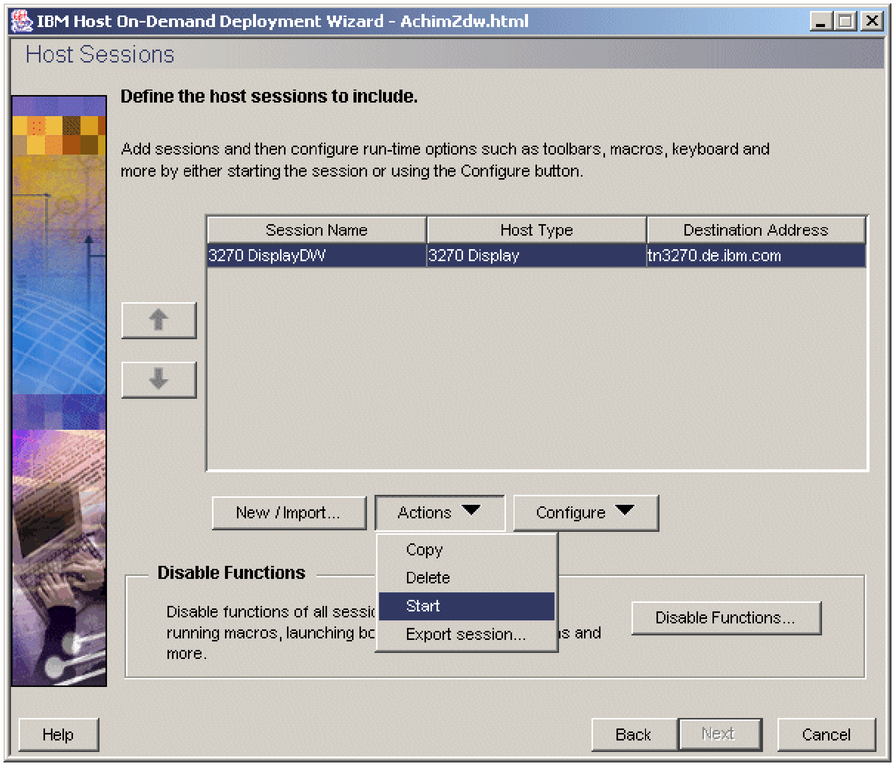
This example will show the following scenario:

The administrator has a session with a macro which he wants to share and to use in a new session.There is no server macro library.

In this example we use the Deployment Wizard and work at the Host on Demand server machine. However, we still will use the ZIP files for distribution as this is a common procedure.

We start Deployment Wizard by clicking at the Windows task bar **Start -> Programs -> IBM WebSphere Host on Demand Deployment Wizard -> Deployment Wizard**.

We chose **Edit an existing HTML** file. From the appearing selection panel we select the **HTML file** which contains our macro. We click through next panels by clicking the **Next** buttons until we reach the panel as seen in Figure 23-9.



Define the host sessions to include.

Add sessions and then configure run-time options such as toolbars, macros, keyboard and more by either starting the session or using the Configure button.

Session Name	Host Type	Destination Address
3270 DisplayDW	3270 Display	tn3270.de.ibm.com

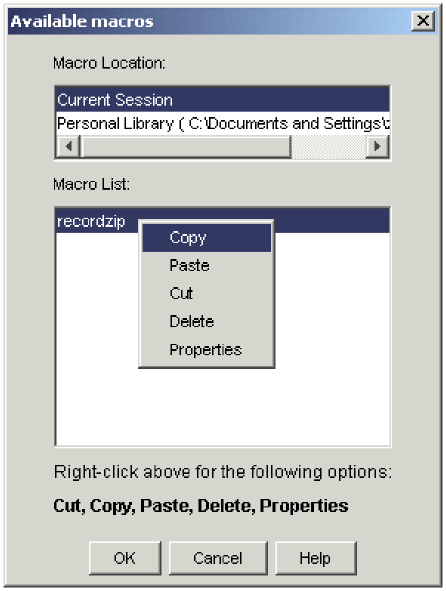
Disable functions of all sessic running macros, launching bc ...s and more.

Figure 23-9 Starting Session from within Deployment Wizard

Here we click the button **Actions** and select **Start** which starts the session.

From the session's menu bar we select **View -> Macro Manager**. The Icon bar for the macro manager is added to the toolbars of the session. We click here at the drop down box for selecting a macro.

The window as shown in Figure 23-10 appears. In the upper window (Macro Location) we select **Current Session** and the Macro List will show the imbedded macros.



Right-click above for the following options:

Cut, Copy, Paste, Delete, Properties

Figure 23-10 Copy a macro from current session

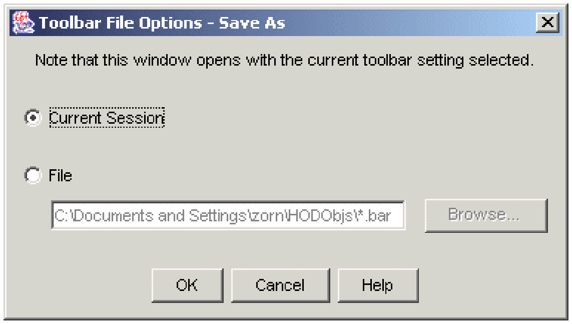
We selected our macro `recordzip` and right-clicked so that the cut and paste submenu as shown in Figure 23-10 is displayed. We clicked **Copy** so that the macro is copied from the current session into the macro clipboard (which is a buffer = similar to windows clipboard).

Now, select in the Macro Location the **Personal Library**, right-click and select **Paste.** By that the macro is copied from the macro clipboard into the subdirectory as indicated in the Personal Library (in our example = `c:\Documents and Settings\zorn\HODObjs`). The macro is saved here as file using the macro name and extension `*.mac` (`recordzip.mac`).

Now you can leave this session and click your way out of the Deployment Wizard. For the new session we again started the Deployment Wizard and created a new HTML file. We used an HTML-based model. Fill in the host type, session name, and address. After that, you will reach the panel as in Figure 23-9. Again, start the session and use the macro manager. Using the cut and paste menu as before, we copied the macro from the Personal Library into the macro clipboard and pasted it from there into the Current Session. Click **OK** and the Macro Manager will show the copied macro in the selection drop down box as the selected macro. Finish the rest of your configuration with Deployment Wizard, save it as zip file, and distribute it to the publish directory of the Host on Demand server using DWunzip. After that this new session, the macro is imbedded in the configuration files, and will be available to the users of that session.

Toolbar

As for the macro we use again the Deployment Wizard and start the session which has the toolbar which we want to use on a new session. From there we use the same procedure as for the toolbar for users explained in Section , “Toolbar and keyboard” on page 828. As for the administrator there is one important additional step to add to that procedure: After the toolbar has been opened and is active in this session, the administrator has to right-click again at the toolbar, select **Save as...** and to save the active toolbar to Current Session, as shown in Figure 23-11. Finish the session configuration and this toolbar will be available for the end users of that session.



Note that this window opens with the current toolbar setting selected.

● Current Session

○ File

C:\Documents and Settings\zorn\HODObjs\*.bar

Figure 23-11 Saving active toolbar to session config

As long as we had not saved the opened toolbar definition within the session, the toolbar was only active for the session as being executed in memory. But the session configuration as stored ion the disk did still contains the previous toolbar configuration as an imbedded definition.

23.5 Scenario using server macro libraries

Administrators can create a library of macro files on the server. Such a macro is only distributed to the user when the user will need it for execution. This is different than the functions of macros in a personal library or toolbar and keyboard definition files, which must be imbedded by the administrator prior to making a session available to the users.

Advantages and features are:

- Easy way to store, edit, and administer macros
- Easy macro sharing across multiple users and multiple sessions
- Reduces size of session configuration files - no need to imbed all potential macros
- Updates of a macro in the library are automatically picked up when a user uses it after the change. There is no need to update the HTML or configuration.
- The server macro library can be configured either as Web or shared drive library.
- When a user launches a session, the macros in the administrator's library will be listed in the macro GUI under "Server Library".
- Available only for sessions defined with the Deployment Wizard (HTML model only)

23.5.1 Example

For this example, assume we have prepared a set of macro files. We put them in the Web server macro library. Then we use Deployment Wizard to create a session that makes those macros available to the users.

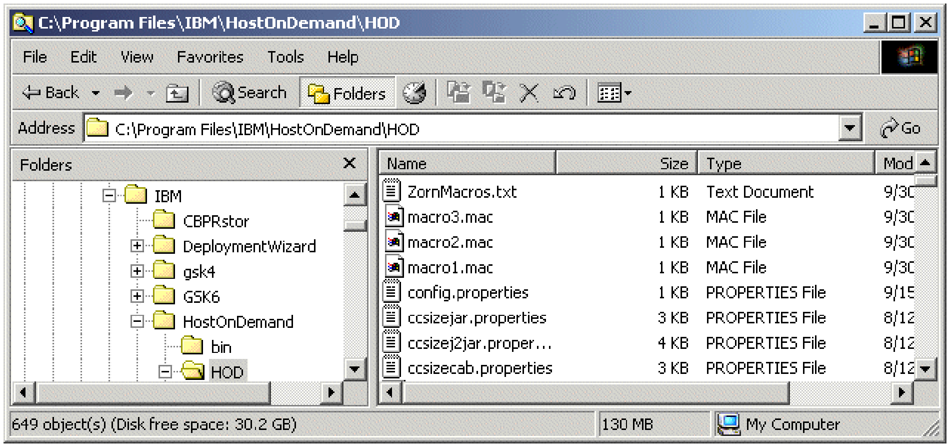
Put macros to Web server macro library

We copied the `*.mac` files to a publish directory on a server. It does not need to be the Host on Demand's publish directory, but we used it that way in the example. Also, we edited a text file (`zornmacros.txt`) which contains the list of macros that we want to make available for this session. You can have several list files. For example, one for 3270 sessions using VM and another one for 3270 sessions using TSO. Each text file contains only the list of macros, which apply to those sessions. In our example, we have only three macros, which all should be available for the new session.

The list file `zornmacros.txt` is a text file edited with Notepad and contains only the following three lines, which make the selected macro files available to any session that includes this server macro library:

```
macro1.mac
macro2.mac
macro3.mac
```

This list (`zornmacros.txt`) must be in the same publish library as the macro files contained in that list. In our example, all are on the Host on Demand publish subdirectory as shown in Figure 23-12.



Name	Size	Type	Mod
ZornMacros.txt	1 KB	Text Document	9/3C
macro3.mac	1 KB	MAC File	9/3C
macro2.mac	1 KB	MAC File	9/3C
macro1.mac	1 KB	MAC File	9/3C
config.properties	1 KB	PROPERTIES File	9/15
ccsizejar.properties	3 KB	PROPERTIES File	8/12
ccsizej2jar.proper...	4 KB	PROPERTIES File	8/12
ccsizecab.properties	3 KB	PROPERTIES File	8/12

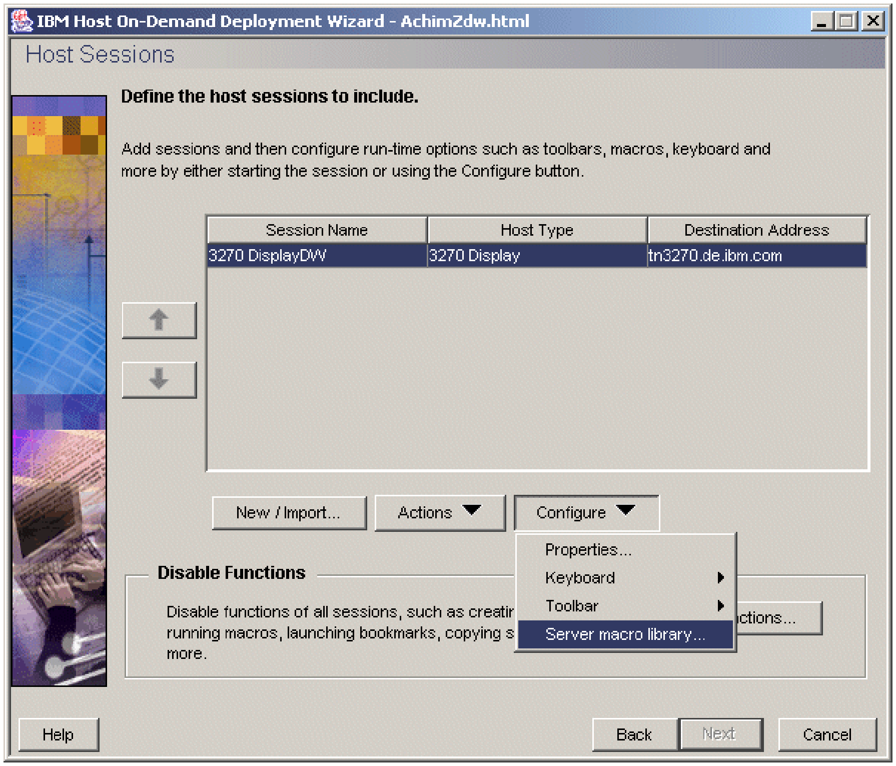
649 object(s) (Disk free space: 30.2 GB) | 130 MB | My Computer

Figure 23-12 Macros and macro list in Web server macro library

The following rules apply to the list file:

- One macro name per line
- Macro name must be the first item on the line.
- Name can start in any column
- Anything after the macro name is ignore, so comments can be added after the name
- Macro name must include the .mac extension
- Blank lines are allowed but are ignored
- Lines starting with “//” are ignored (can be used for comments)
- List file must be in the same directory as the listed macros

Now, we started the Deployment Wizard, and started configuring a new HTML based session. After we have created it by entering session name and destination address, we added the server macro library: At the Host Session panel of the Deployment Wizard we clicked **Configure** and then **Server Macro Library** as shown in Figure 23-13.



IBM Host On-Demand Deployment Wizard - AchimZdw.html

Host Sessions

Define the host sessions to include.

Add sessions and then configure run-time options such as toolbars, macros, keyboard and more by either starting the session or using the Configure button.

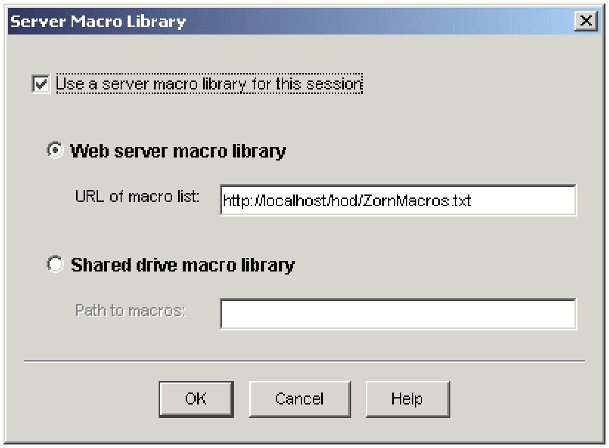
Session Name	Host Type	Destination Address
3270 DisplayDW	3270 Display	tn3270.de.ibm.com

Disable Functions

Disable functions of all sessions, such as creatir running macros, launching bookmarks, copying s more.

Figure 23-13   Add server macro library

The panel Server Macro Library is displayed. Here we selected the check box **Use a server macro library for this session**, selected the radio box **Web server macro library,** and entered the URL of our macro list file as shown in Figure 23-14.



☑ Use a server macro library for this session

● Web server macro library

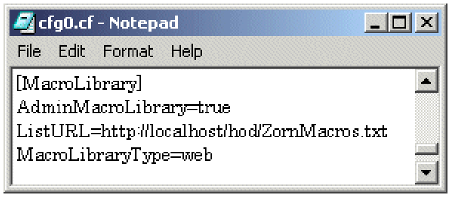
URL of macro list: http://localhost/hod/ZornMacros.txt

○ Shared drive macro library

Path to macros:

Figure 23-14 Entering name of Web server macro library

The resulting configuration file which will be generated later by DWunzip will show those parameters in the MacroLibrary stanza in the cf file of this session. See Figure 23-15. You will notice that no macros are listed or imbedded. Only the macro list file is referenced.



```
[MacroLibrary]
AdminMacroLibrary=true
ListURL=http://localhost/hod/ZornMacros.txt
MacroLibraryType=web
```

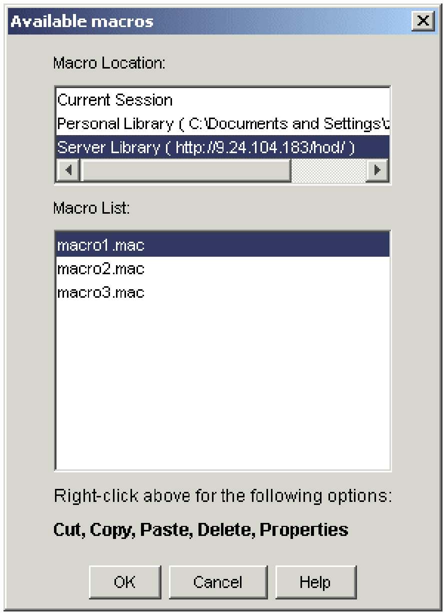
Figure 23-15 MacroLibrary stanza in cf file

Now we continue to finish the configuration using the Deployment Wizard. We chose **Java Auto Detect** and **Download Client** and created the zip file.

After finishing the configuration, we copied the resulting zip file to the publish directory of the server. Then we used DWunzip to generate and distribute the configuration files to the publish directory for usage by the clients.

If the Deployment Wizard is running at the same machine as the Host On-Demand server, you can create the HTML files instead of using ZIP and DWunzip. In that case, make sure the output directory for saving the HTML file points to the Host On-Demand publish directory (default of Deployment Wizard is the `DW \hoddata\ subdirectory`).

Now open the HTML of the new session in the client. The session will appear in the browser window. View the macro editor and click its pull -down box to open. Here we selected the **Server Library;** see the macros that are listed in the macro list as shown in Figure 23-16.



Available macros

Macro Location:

Current Session
Personal Library (C:\Documents and Settings\
Server Library (http://9.24.104.183/hod/)

Macro List:

macro1.mac
macro2.mac
macro3.mac

Right-click above for the following options:

Cut, Copy, Paste, Delete, Properties

Figure 23-16 Macros of Server Library

From this list you can choose a macro to be inserted into the Selected Macro drop down box for execution. We also can use the macros with the macro clipboard, for example, you can copy a macro from the server library and paste it into the current session. A macro in the current session will appear with its macro name. So, if the macro file `macro1.mac` contains a macro named `xyz`, the current session shows `xyz` as a pasted macro name. You should always have the same name for the file name and the macro name to avoid confusion.

23.5.2 Common problems

If you are not seeing the list as shown in Figure 23-16, check your Java console and look for errors:

```
ERROR: Macro library list: http://9.24.104.183/hod/zornmacros.txt was not found
```

If so, is the name listed in the error message the correct filename? Check also the filename in the cf file. Check the file name again in the Deployment Wizard by editing the HTML using Deployment Wizard. If you start the session from within the Deployment Wizard while editing, does it work here? Possible errors are wrong filename, wrong subdirectory name, the subdirectory is not published, the HTML files have not been properly copied from Deployment Wizard to Host on Demand publish subdir, or (in case of zip files) you have mixed up the files for saving, DWunzipping, or copying from Deployment Wizard to Host on Demand server:

```
ERROR: Macro not found:  http://9.24.104.183/hod/macro1.mac
```

In this case, select (from Figure 23-16) **macro1**. The macro list file did contain this entry so that it appeared for selecting. But, a macro file with that name (or with the extension .mac) did not exist in the server macro library subdirectory. Make sure that all macros as listed in the list file exist in the same subdirectory, and all have the extension .mac.

23.5.3 Deploying a server macro library to a shared drive

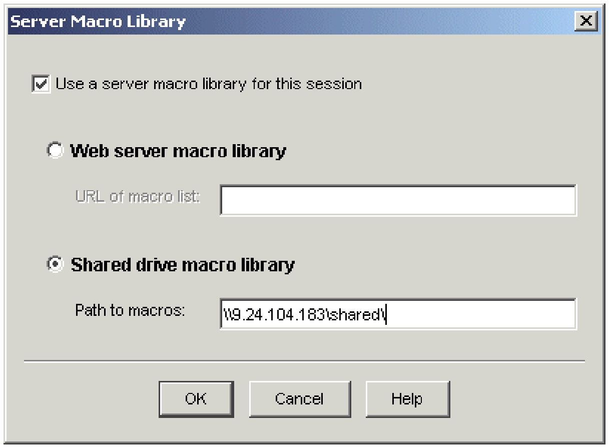
Analog to the Web macro library you can set up the same functionality for drives and paths shared on a LAN. Take the following steps for configuration and usage:

1. Put your macros in a shared directory on your network. Examples of valid directories include the following:
   - Absolute paths. Mapped network drive letters can also be used in the absolute path. Note that a server macro library should never point to a local drive.
   - Remote computer names or IP addresses are allowed as long as the user’s computer is already remotely connected and authenticated to the computer that is sharing the directory. The following are two examples of paths to share drive macro libraries:
     - \\your_host\macro_library, where your_host is the host name, macro_library is the macro directory
     - \\123.45.67.89\macro_library\, where 123.45.67.89 is the IP address of the host, macro_library is the macro directory

   If you are configuring a macro library for more than one session, and each session uses its own set of macros, you will need to create a separate directory for each session.
2. In the Deployment Wizard Host Sessions window, select the session you wish to configure, click the **Configure** menu, and select **Server macro library**.

Check the **Use a server macro library for this session** box and select **Shared drive macro library**.

3. Specify the directory path that you set up in Step 1. See Figure 23-17 as an example.



☑ Use a server macro library for this session

○ Web server macro library

URL of macro list:

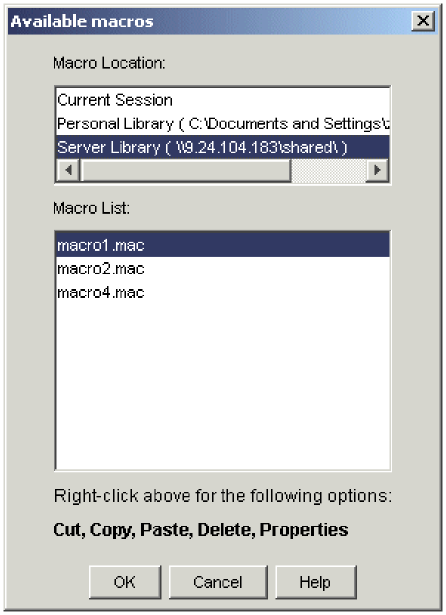
● Shared drive macro library

Path to macros: \\9.24.104.183\shared\

Figure 23-17 Shared Macro Library setup

4. Click **OK**.

When users open their sessions, they can use the **Play Macro** or the **Available Macros** windows to see a list of the macros in the directory. These macros are available when users select **Server library** as their macro location. See Figure 23-18 as an example. The Server library location is only available if you have configured the session to use a server macro library.



Available macros

Macro Location:

Current Session
Personal Library (C:\Documents and Settings\
Server Library (\\9.24.104.183\shared\ )

Macro List:

macro1.mac
macro2.mac
macro4.mac

Right-click above for the following options:

Cut, Copy, Paste, Delete, Properties

*Figure 23-18 List of available *.mac files in subdirectory of a shared macro library*

24

Host Access Toolkit

The HACP 4.0 Host Access Toolkit contains a set of Java libraries with which developers can create applets and applications for host access. The set of application programming interfaces (APIs) is a separate stand-alone product from Host On-Demand (HOD). It is bundled with Host On-Demand and is part of the Host Access Client Package, but shipped on its own CD. The toolkit can be installed and deployed independently of Host On-Demand.

In this chapter, we discuss how to use these libraries in today's real-world development and production environments. A previous redbook *Programming with the Host Access APIs,* SG24-5856, is available as an introduction to the structure of these libraries and how to get started developing with them. This chapter will serve mainly as an extension and revision to the more recent redbook, *IBM Host Access Client Package,* SG24-6182-01.

The following libraries are discussed in this chapter:

- Host Access Class Library for Java (HACLJ)
- Host Access Beans for Java (HABJ)
- J2EE Connectors

The free-for-downloading EHLLAPI Bridge and Utility technologies are also discussed.

If you only want to re-arrange the appearance of the Host On-Demand desktop, use the Programmable HOD feature introduced in Host On-Demand V8 instead of APIs from Host Access Toolkit. The Programmable Host On-Demand API is a set of Java APIs that allows developers to integrate various pieces of the Host On-Demand client code, such as terminals, menus, and toolbars, into their own custom Java applications and applets. For more information, refer to *Programmable Host On-Demand* document in the Host On-Demand V8 Infocenter:

```
http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/
```

24.1 Introduction

In this release of the Host Access Toolkit, the associated APIs contain extensions and improvements. The related Personal Communications associated Java APIs remain at the same version as the last release of the Host Access Client Package. Those APIs are equivalent to HOD 4.3.

The following are new features for Host Access Class Library for Java (HACLJ):

- The ECLSession and ECLConnection classes now include methods to enable or disable support for the display of Unicode data in 5250 Display sessions:
  - OS/400 V5R2 supports display of Unicode characters using Coded Character Set Identifiers (CCSID).
  - Host On-Demand Version 8.0 supports this feature on 5250 Display Sessions.
- The package ECL has been extended to support Secure SHell (SSH) on VT sessions. This release supports a subset of SSH version 2.0 protocol. For more detailed information on the SSH protocol, please refer to IETF Secure Shell (secsh) Charter home page at:

  ```
  http://www.ietf.org/html.charters/secsh-charter.html
  ```

  - Java 2 and Java Cryptography Extension (JCE) are required to run SSH in HACL. JCE is included in Java 1.4 and later.
  - SESSION_SECURITY_PROTOCOL must be set to SESSION_PROTOCOL_SSH.
- The ECLSession class now includes several properties for Web Express Logon (SSO_).
- The ECLPS class now includes MagStripeReader and BadgeReader methods, each with three method signatures. These methods allow Host On-Demand to handle Magnetic Hand Scanners, Magnetic Card Readers, and Optical Scanners in 3270 sessions as described in *3270 Information*

Display System Data Stream Programmer's Reference, GA23-0059-07, “Chapter 7.”

- For bidirectional support, methods were added to support bidirectional processing for methods like GetString, SearchString, and SetText. These methods are available through the ECLPSBIDIServices interface for 3270 Display and 5250 Display sessions, and through the PSVTBIDIServices interface for VT Display sessions.
- The ECLSession class and the ECLConnection class now include methods for specifying backup Telnet servers. These methods let you specify up to two backup servers (along with LUs/pools and ports) for the following session types: 3270 Display, 3270 Printer, 5250 Display, and 5250 Printer, CICS Gateway client, and VT Display.

The following are new features for Host Access Beans for Java (HABJ):

- The Session bean and the terminal bean support the display of Unicode data on 5250 Display sessions:
  - OS/400 V5R2 supports display of Unicode characters using Coded Character Set Identifiers (CCSID).
  - Host On-Demand Version 8.0 supports this feature on 5250 Display Sessions.
- For Java 2 only, the Session bean and terminal bean have been extended to support Secure SHell (SSH) on VT sessions. This release supports a subset of SSH version 2.0 protocol. For more detailed information on SSH protocol, please refer to IETF Secure Shell (secsh) Charter home page at:

  `http://www.ietf.org/html.charters/secsh-charter.html`
- The session bean now includes several properties for Web Express Logon.
- The ECLPS bean now includes MagStripeReader and BadgeReader methods, each with three method signatures. These methods allow Host On-Demand to handle Magnetic Hand Scanners, Magnetic Card Readers, and Optical Scanners in 3270 sessions as described in *3270 Information Display System Data Stream Programmer's Reference,* GA23-0059-07, “Chapter 7.”
- The HostPrintSession bean now includes the following boolean properties for bidirectional support: RTL_FILE, SYMMETRIC_SWAP, NUMERIC_SWAP.
- The following new classes have been added as extensions to the MacroAction class:
  - MacroActionPrintStart
  - MacroActionPrintExtract
  - MacroActionPrintEnd

- The Terminal, Session, and HostPrintTerminal beans now include methods for specifying backup Telnet servers. These methods let you specify up to two backup Servers (along with LUs/pools and ports) for the following session types: 3270 Display, 3270 Printer, 5250 Display, and 5250 Printer, CICS Gateway, and VT Display.
- The material previously in “Appendix A: Macro Script Syntax” has been rewritten and moved to the regular online documentation provided with IBM WebSphere Host On-Demand Version 8.0. The document is the *Host On-Demand Macro Programming Guide,* SC31-6378.

> **Note:** The term *application* is used loosely in this document. Unless explicitly stated, an *applet* is also inferred. In some topics, both terms will be used. Application refers to a Java program launched through the *main* entry point, while applet refers to Java code launched in a browser environment through the *init* entry point.

24.2 Host Access Toolkit requirements

Installing and using Host Access Toolkit has some requirements that must be met in terms of the supported operating systems, disk space requirements, Java 2 support, and the types of browsers. This section explains each of these requirements.

24.2.1 Operating systems requirements

The installation of the toolkit and development of applications is supported on the following operating systems:

- Windows 95
- Windows 98
- Windows Me
- Windows NT 4.0 with service pack 3 or higher (SP 6a is recommended)
- Windows 2000
- Windows XP

Applications developed using the Host Access Toolkit can be run on other operating systems that support Java. The toolkit JAR files needed to run your application or applet can be packaged with your application or applet, and copied to those other systems within the bounds of your licensing agreement.

The typical Host Access Toolkit requires 126 MB of disk space to install.

Supported browsers

The following browsers can be used to run a Host Access Beans for Java or Host Access Class Library applet:

- Netscape Navigator 4.7 and 6.1, 6.2, 7.0 (Windows 95, Windows 98, Windows NT. Windows 2000, Windows XP, UNIX)
- Netscape Navigator 4.6.1 (IBM OS/2) and IBM Mozilla Web Browser for OS/2
- Microsoft Internet Explorer 4.01 with SP1, 5.0, 5.1, 5.5 and 6.0 with their most current service packs

> **Note:** As of this writing, there is a special situation for users of Internet Explorer on Windows XP. The details are presented here:
>
> `http://www.microsoft.com/windowsxp/pro/evaluation/news/jre.asp`

- Mac OS X Safari
- Mozilla 1.0.2, 1.2.0, 1.2.1, 1.3
- Other browsers that support the Java Runtime Environment (JRE) 1.3 Plug-in or later

For the most up-to-date information, refer to the read me file and visit the Host On-Demand Web site.

24.2.2 Supported target environments

IBM supports developing applications derived from the Host Access Toolkit for the following platforms, JREs, and browsers (for applets).

Platforms

Supported platforms encompass Windows, IBM mainframe, IBM midrange, and UNIX platforms.

- Windows: 95*, 98, NT 4.0, 2000, ME, XP**
- OS/2
- IBM OS/400
- IBM OS/390
- IBM AIX
- Linux
- Sun Solaris
- HP/UX

Note: Supported target Windows platforms vary according to the JVM release.

*IBM JVM 1.3.1 and above will not launch on Windows 95. In contrast, Sun JVMs up to 1.4 are supported for Windows 95. Please consult the java.sun.com Web site for specific details on supported platforms.

**IBM JVM 1.1.8 and 1.3.0 are not supported on Windows XP (but may work).

Java Runtime Environment (JRE)

We discourage development of API-based software using JDK 1.1.8 and JDK 1.2, although it is certified for those levels. Only limited maintenance should be done with JDK 1.1. Version 1.1.8 is close to going out of service with the specific dates depending on the platform. Look forward to Java 2 V1.3.x and beyond for new development, keeping future V1.4 requirements in mind.

IBM JREs/JDKs should be used in conjunction with these libraries. You may download one from:

http://www.ibm.com/developerworks/java/jdk/index.html/

Select the **IBM Developer Kits** option and then select the appropriate operating system. The Java Plug-in is in the Windows package and installed by default.

24.3 Host Access Toolkit versus Personal Communications

Personal Communications (PCOMM) also contains HACLJ and HABJ API libraries. However, their functionality and features are at the level found in Host On-Demand V4.0. Source code developed in the PCOMM Java API library environment will generally compile and run in the HOD Java API jdk1.1 library environment. A specific exception to this are the HACL screen recognition classes: the flow logic for PCOMM usage is different than the flow logic for HOD 8.0.

Personal Communications ships with additional APIs to support Win32-specific development using programming languages such as Microsoft C++, Microsoft Visual Basic, and Lotus Notes. For this chapter it is very important to contrast the Java libraries supplied by Host On-Demand 8.0 and Personal Communications.

The Java libraries supplied in the Host On-Demand Toolkit are written 100% in Java, and can be executed in a platform-independent manner. The Host On-Demand product does not have to be installed on the client machine. The entire functionality of HACLJ and HABJ is contained in the supplied JAR and CAB files. These JARs/CABs are installed on the local machine in the case of an application. They may be locally installed or downloaded from a server in the case of a browser-based applet.

The Personal Communications product is Windows- and OS/2-specific. The Personal Communications version of HACLJ and HABJ functionality is absolutely dependent on the presence of the Personal Communications emulator product being installed on the local machine. In fact, sessions created with HACLJ or HABJ work by starting a hidden Personal Communications emulator session(s). Portions of the HACLJ library are wrapper classes for Java Native Interface (JNI) access to this hidden Personal Communications session(s).

Host On-Demand-based HACLJ and HABJ are Java right down to the transport layer. In contrast, the Personal Communications version is largely Java, but the “transport” layer is the Personal Communications product itself.

The Host On-Demand Toolkit contains a variety of JARs/CABs to supply host access functionality (`habasen.jar`, `ha3270n.jar`, and others). Personal Communications only ships one JAR, pcseclj.jar, and no corresponding CAB file. CAB files are the primary library and security mechanism for running Java applets using MS Internet Explorer. Netscape uses JAR files. Therefore, the Java libraries supplied with Personal Communications are not intended and not supported for browser-applet usage. They should be used in stand-alone applications only.

24.4 Host Access Class Library for Java (HACLJ)

Traditionally, specialized terminal equipment was used so that the user could communicate and interact with several kinds of host computer presentation screens: 3270, 5250 or VT (ASCII virtual terminal). The advent of the multi-purpose Personal Computer ushered in terminal emulation software. The Java-based Host On-Demand emulator product is an example. Host On-Demand itself is based on Host Access Beans for Java plus considerable value-added glue logic to simulate an advanced terminal emulator. The Host Access Beans, in turn, rely heavily on the Host Access Class Library for Java.

Note: The HACLJ objects begin with ECL. The Host Access Class Library was originally called the Emulator Class Library (ECL), but the name HACL was deemed more appropriate. The actual code bindings maintain their original acronym of ECL.

24.4.1 HACLJ programming strategy

HACL for Java provides a non-visual API for interacting with back-end host machines running applications originally designed for human interaction. Human-oriented host applications relied on readable character presentation, formatted fields, color-coding, and keyboard responses. The HACLJ library provides specialized classes for functionalities needed to mimic traditional human interaction with a series of host screen presentations (“green screens”). HACLJ contains no GUI (visible component) classes. The HACLJ classes interact with “invisible” presentations screens. HACLJ provides the PSDebugger, a simplified terminal that appears on demand by issuing `ECLSession.ShowPSDebugger(true)`.

A client side HACLJ-based application can simply be a straightforward replacement for a repetitive routine. There is no direct need for a terminal screen or decision-making by the operator. This most resembles a batch program.

Another application type deploys a remapped, reformatted, or blended presentation of the information content extracted from one to several host screens and databases. The developer may create an application where the user may be completely unaware of the connection to the mainframe. The user does not need to learn the special procedures, commands, or menu structure of the host application; these can be automated by a domain expert using HACLJ. As a result, the user can focus more on the task at hand. The HACLJ portion of the application is in complete control of host screen navigation, so if the host side presentation content changes, so must the navigation and recognition logic. The user interacts only with the business logic presented. What used to be done as a series of discrete steps sequentially to move and manage data between several hosts can be turned into a single flow of steps among multiple hosts simultaneously.

In addition to client-side development, one can develop an application in a middle-tier solution for host access. One such example is to create an EJB, or servlet, that utilizes HACLJ to do transactions for a user, such as a Web site to a bank. Here again, the HACLJ code is replacing what would have been human interaction with a remote mainframe back-end. The middle tier functionality receives commands through the Web and translates them into HACLJ-mediated trains of action. Back-end responses are screen scraped and transcoded into Web page-based replies. Some of this work has already been done for you by supplying the J2EE Connectors as part of the toolkit. The choice is simple: would you rather have a client machine or a middle-tier application server accessible to a client performing host navigation and screen scraping? Figure 24-1 demonstrates these concepts.

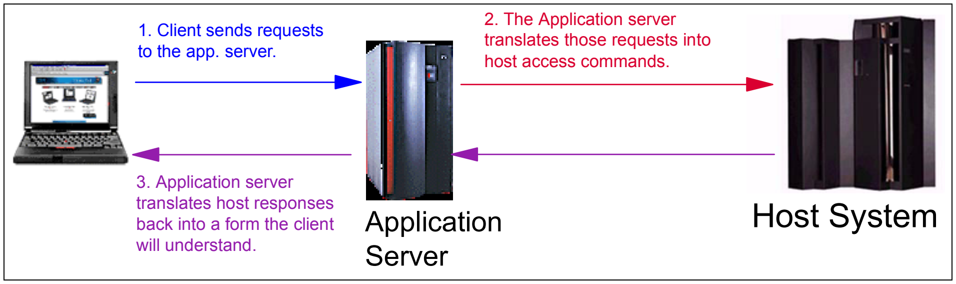

1. Client sends requests to the app. server.
2. The Application server translates those requests into host access commands.
3. Application server translates host responses back into a form the client will understand.
Application Server
Host System

Figure 24-1 Application server with Host On-Demand J2EE Connectors

24.4.2 HACLJ functionality

Table 24-1 presents most of the higher-level functions that can be programmed using HACLJ.

Table 24-1 HACLJ functions and associated objects

Functionality	**Associated objects in HACL**
Important Global Constants	ECLConstants - used with HACLJ and HABJ
Session	ECLSession - communicates with host, derived from ECLConnection ECLConnection - connects to host ECLCommNotify - communication events listener interface
Presentation Space	ECLPS - logical representation of the Presentation Space (PS) or "green screen" ECLPSEvent - PS change notification event ECLPSListener - PS change notification listener interface ECLFieldList - logical representation of all of the fields present in the PS ECLField - logical representation of a single field within the PS
Operator Information Area (OIA)	ECLOIA - logical representation of the operator information area (OIA) ECLOIANotify - OIA change of state listener

Functionality	Associated objects in HACL
File Transfer	ECLXfer - allows the transfer of files to and from a 3270 or 5250 host, over an established session. ECLXfer supports the 3270 Host File Transfer Program IND$FILE (for SBCS) or APVUFILE (for DBCS) transfer protocols, which can be controlled by means of the standard IND$FILE or APVUFILE send and receive options. ECLXfer also supports 5250 File Transfer, which can be controlled by means of the send and receive options specific to OS/400. ECLXferEvent - fired to notify listeners of progress during file transfers. ECLXferListener - interface can be used to implement an object which will receive the file transfer progress events, ECLXferEvent. Events are generated during file transfer as data buffers are transferred to or from the host.
Printer Session Control	ECLHostPrintSession - can be used to establish a print connection with a host. This class defines the behavior and characteristics of the print session with the host. This class inherits operating characteristics and behaviors from its parent class ECLSession. Like ECLSession, ECLHostPrintSession can be constructed with a Properties object which contains all the configuration information for the print session. Configurable information includes the session type (3270 printer session or 5250 printer session), PDT file name and port number. ECLPrintJobEvents - are fired by ECLHostPrintSession to notify interested listeners about a current print job. There are several event types that coorelate to the nature of a print job state change or an error condition occurrence. Some event types contain additional information. ECLPrintJobListener - interface can be used to implement an object which will receive ECLPrintJobEvents. Events are generated whenever a printer job is started or completed. Special events are generated when print job related errors occur.

Functionality	Associated objects in HACL
National Language Version Extensions	ECLPSBIDIServices - interface provides access to the bidirectional (BIDI) language properties in an ECLPS object. An ECLPSBIDIServices object is only available when using bidirectional code pages (420, 424, or 803) in 3270/5250 Sessions. ECLPSTHAIServices - interface provides access to the THAI properties in a THAI ECLPS object. An ECLPSTHAIServices object is only available when using Thai codepages (838 or 1160) in 3270, 5250 and VT sessions. ECLXferBIDIServices - interface provides access to the ECLXfer Bi-directional (BIDI) Language properties in an ECLXfer object. An ECLXferBIDIServices object is only available when using Bi-directional code pages (420, 424, or 803). PSVTBIDIServices - interface provides access to the bidirectional (BIDI) language properties in a BIDI VT session. The PSVTBIDIServices object is only available when using bidirectional code pages.

Functionality	Associated objects in HACL
Screen Recognition	ECLScreenDesc - a target screen “described” through specialized descriptors ECLScreenReco - the screen recognition engine ECLRecoNotify - called when screen recognition engine “recognizes” a described screen ECLSDAttrib - describes a single attribute on a host screen ECLSDBlock - describes a block of strings on a host screen ECLSDCursor - describes the cursor position on a host screen ECLSDCustom - describes a custom recognition handler for a host screen ECLSDFields - describes the total number of fields on a host screen ECLSDInputFields - describes the number of input fields on a host screen ECLSDOIA - describes an OIA condition to wait for after a host screen is recognized ECLSDString - describes a single string on a host screen ECLSDScreenDescriptor - is the base class that all ECLSD* classes are derived from ECLCustomRecoEvent - emitted after standard screen matching logic for “final approval of match” ECLCustomRecoListener - an interface to extend the base ECLScreenReco screen matching logic ECLRecoDebugEvent - debug event emitted upon screen recognition occurrence ECLRecoDebugListener - debug event listener interface
API Error Event	ECLErr - error event classes specialized to HACLJ VariableException - is thrown when problems with Macro variables and arithmetic expressions are encountered. VariableException objects are created and populated with error and diagnostic information, and then thrown as exceptions. The VariableException object can then be caught and queried for the error information. VariableException is informational for Macro bean programming only.
Outboard Function Execution	ECLAppletInterface - access to currently running ECLSession

Functionality	Associated objects in HACL
Trace Facility	ECLTrace - base of trace facility in HACLJ ECLTraceEvent - emitted to transmit internal state and progress information ECLTraceListener - trace event listener interface ECLTraceProducer - interface implemented by an HACLJ component reporting trace information

For full details, please refer to the online *Host Access Class Library Reference*.

24.4.3 Automated host navigation

The Host Access Toolkit provides several assistive technologies to help applications navigate screens. These technologies can minimize the amount of work spent developing the screen-to-screen flow needed to perform the required business logic of an application. An all-HACLJ application would use the screen recognition API of HACLJ. Usually, a HABJ-based application would use the Macro or MacroManager beans. However, Session and Terminal beans both provide access to ECLPS through ECLSession, so that the HACLJ screen recognition API can be used in an HABJ application.

Screen recognition in HACLJ

Screen recognition, or screenreco, provides an event-driven model for recognizing a particular host screen among a succession of screens presented. Using the respective classes enumerated in the table above, a developer defines one or more properties that will be used to "match" a screen. A set of descriptors must uniquely identify the target screen, especially when there are other "similar" screens that can also be reached in a non determinate traversal situation. The programmer must also account for screen completeness; there is no formal data stream signal to announce that the host has completed updating the screen. That requires judgment and experience on the part of the developer of the recognition criteria. Here are the properties that can be formed into various combinations for a unique match:

- Attribute byte of a field
- A unique string and position
- A block of strings
- The cursor position
- The number of fields on the screen
- The number of input fields
- An OIA condition to wait for after a host screen is recognized

These may not be enough when the same static screen layout is progressively updated in response to user inputs. Each of those updates may represent new states to be recognized in the business logic. Therefore, a fine differentiation is possible by using the “custom reco” facility based on:

- ECLSDCustom

  Describes a custom recognition handler for a host screen
- ECLCustomRecoEvent

  Emitted after standard screen-matching logic for “final approval of match”
- ECLCustomRecoListener

  An interface to extend the base ECLScreenReco screen-matching logic

The screenreco engine triggers on each presentation space update (keyed to ECLPSEvent occurrence). A screen matches when a defined cluster of criteria is fulfilled. A reco event is fired to any registered listener. For more information, including examples, see *Programming with the Host Access APIs*, SG24-5856.

Known limitation

When ECLScreenReco is used with Terminal/Screen in the Personal Communications version, there is an unavoidable performance limitation. When a skilled touch typist reaches top speed, occasional keystrokes are not echoed to the screen. No keystrokes are lost from the input buffer of the virtual terminal. All keystrokes reappear when the presentation space is manually refreshed.

HACLJ suited to all platforms

All supported platforms can take advantage of HACL for Java because the platform does not need to provide a GUI engine. This can be eased a bit with Remote Abstract Windows Toolkit (RAWT), also called Remote AWT.

Timing

Host programs might be designed to indicate when a refreshed presentation is complete, but data stream protocols do not have a formal signal that a screen update has been completed. HACLJ itself does not relieve the programmer of doing a correct and full analysis of host program and communication link timing behavior.

Where am I?

The screenreco facility is a great aid for systematizing and automating the navigation of a series of host presentation screens. Nonetheless, secondary confirmation that the screen currently presented is the screen expected is absolutely essential. No less important is a strategy to gracefully fall back or withdraw when navigational expectations do not match reality.

Beep

The 3270 “bell” is sounded when a connection to a host succeeds. The 5250 “alert” is sounded when the OS presents a momentary overriding screen message. The Java JVM provides an equivalent Toolkit.Beep(), which HACLJ uses to provide an “audible.” When the HACLJ-based Java application is running on OS/390 or OS/400, that Toolkit.beep() call has the effect of stalling ECLPSEvents. The symptom is that the connected host appears not to be sending updated screen buffers.

There are two ways to avoid this.

- Quiet Mode

  The ECLSession can be parameterized with the value pair: `ECLSession.SESSION_QUIETMODE`, "true". This is valid for 3270 and 5250.

- Remote Abstract Windows Toolkit (RAWT)

  Full details concerning RAWT are to be found in the article *Setting up the Remote Abstract Window Toolkit for Java on a remote display,* and its associated links at:

  `http://publib.boulder.ibm.com/pubs/html/as400/v4r4/ic2924/info/java/rzaha/devkit.htm`

24.5 Host Access Beans for Java overview

Unlike HACLJ, Host Access Beans (HAB) for Java are intended for visual environments, with the exception of the Session and Macro beans. Developers can present to the user different pieces of an emulator to quickly provide core functions one might expect. The Terminal and Screen beans display the actual screens and OIA information generated by the back-end host. Because Host Access Beans for Java are components themselves, rapid development of applications based upon this library is possible. If the API of the beans is not sufficient for an application’s needs, the underlying HACL for Java API is accessible.

Applications constructed from the visual HAB for Java do not have a place in the middle-tier host access solution. But the Session bean wired with Macro bean is a potent combination in an Enterprise Java Bean servlet environment. HAB for Java provides the greatest benefit when developing client-side solutions for host access, but do not forget that these solutions can either be installed locally on a machine, or downloaded from a Web server to reap the benefits of a single deployment location. Consider Host On-Demand as a model for this.

The Host Access Beans for Java (HABJ) provide core components that can be used to develop an entry-level terminal emulator.

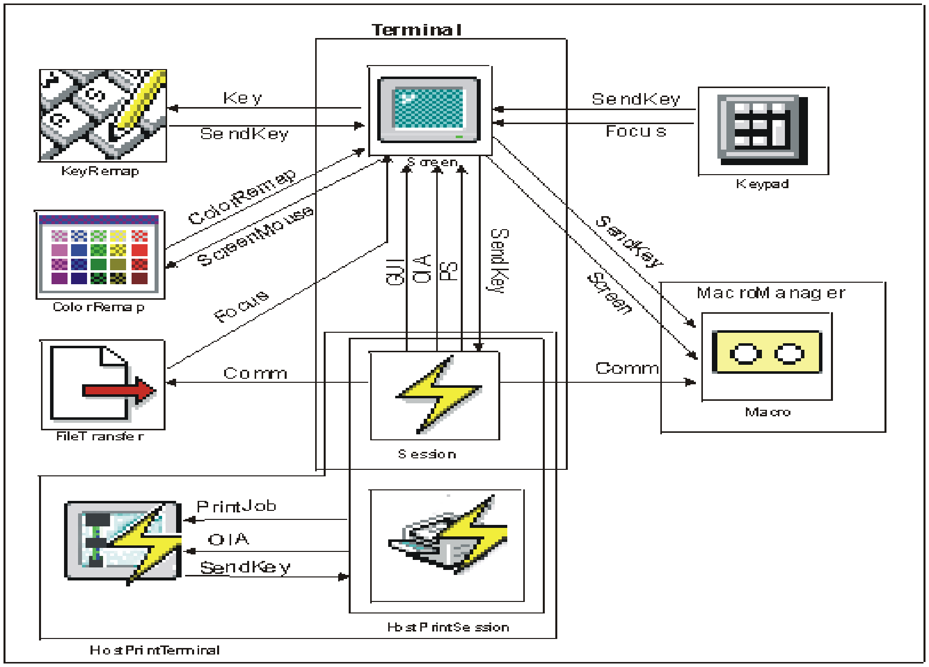


Figure 24-2 Host Access Beans for Java overview

However, wiring the HABJ components together will not provide all of the functionality and usability of the Host On-Demand sophisticated emulator. The purpose of the Host Access Beans is to provide developers with an elementary set of GUI and emulator sub functions that are sufficient to support the main business logic and presentation needs of the deployed custom application. The deployed application should only need elementary host GUI presentation to guide the human user. A custom application that needs the full value-add functionality of an advanced terminal emulator should be designed to use Host On-Demand directly and its RunApplet facility.

The beans available in Version 8.0 of the Host Access Toolkit are listed in Table 24-2.

Table 24-2 Host Access Beans for Java

Icon	Description
Session ⚡	Session is a non-visual bean that provides methods and properties for setting up and establishing communications with the host system. The Session bean fires events that allow listeners to be notified of presentation space, operator information area (OIA), and communication changes.

Icon	Description
Screen	Screen is a visual bean that provides the graphical interface for displaying the host data from a Session bean. The Screen bean listens to presentation space, OIA, and GUI events fired by the Session bean and interprets the events to display the main Presentation Space (“green screen”) and the operator information area (OIA). It fires keystroke events to registered listeners, and also provides the clipboard cut, copy, and paste functions, and controls screen display settings for the codepage, fonts, 3D borders, cursor, and so forth.
Terminal	Terminal bean is a visual bean that combines the Session and Screen beans to provide a composite bean that encompasses both the communication with the host and the graphical interface for displaying the host data.
Keypad	Keypad is a visual bean that provides a simple grid of buttons representing specialized keys that invoke various host functions.
KeyRemap	KeyRemap is a visual bean that provides keyboard remapping capability. Using KeyRemap, keystrokes can be mapped to alternate characters, strings, macros, or directly to host functions.
FileTransfer	File Transfer is a visual bean that provides a toolbar interface for transferring files to and from a host.
Macro	Macro is a nonvisual bean that records and plays a single macro. Macro employs advanced screen recognition technology to reliably navigate host applications in any environment. Macro also provides the ability to prompt for user input and extract text from the screen during playback.
MacroManager	MacroManager is a visual bean that provides a toolbar interface for managing multiple macros. It allows you to record, play, load, delete, and edit macros.
ColorRemap	ColorRemap is a visual bean that provides a simple interface for modifying the colors displayed by the Screen or Terminal beans. The ColorRemap bean is only supported in Host On-Demand.
Host Print Session	HostPrintSession is non-visual bean that extends the Session bean and provides a simple interface for creating and customizing 3270 and 5250 printer sessions.

Icon	Description
HostPrint Terminal	HostPrintTerminal extends the HostSessionBean and provides a simple interface for creating and customizing 3270 and 5250 printer sessions. At run-time, the HostPrintTerminal bean visually displays information about the status of the print jobs and the connection with the host.
Converter	The Converter beans performs codepage-to-codepage conversion. For the Arabic and Hebrew languages, Converter performs certain BIDI-specific transformations, including logical-to-visual transformations, and Lam-Alef processing (Arabic only).

24.5.1 Host Access JavaBeans explained

This section describes the above-mentioned beans in detail.

Session bean

This is a non-visual bean and has a customizer. It provides methods and properties for setting up and establishing communications with a host system and fires events that notify listeners of presentation space (PS), operator information area (OIA), and communication changes. It determines the behavior and characteristics of the session with the host through its properties, which include the session type (3270, 5250, and VT), host, port, session ID, PS size (for example, 24 rows by 80 columns), and the host code page.

Screen bean

This is a visual bean and has a customizer. It provides the graphical interface for displaying the host data from a Session bean. The Screen bean listens to PS, OIA, and GUI events fired by the Session bean and interprets the events to display the main text area and the OIA. It fires keystroke events to registered listeners, and also provides the clipboard cut, copy, and paste functions.

This bean is sensitive to both the session type and code page and has different behaviors for the different session types and for single-byte, double-byte, and bi-directional code pages. The OIA displays different information according to the session type and code page.

Among its properties are:

- The sessionType property that affects its display of host data. The sessionType property is an enumeration for which the valid values are 1 for 3270, 2 for 5250, 3 for VT, and 4 for CICS.
- The oiaVisible boolean property. This causes the OIA to be turned on or off.

Terminal bean

This visual bean combines the Session and Screen beans to provide a composite bean that encompasses both the communication with the host and the graphical interface for displaying the host data.

Keypad bean

This visual bean provides a simple grid of buttons that invoke various host functions.

A user can execute keyboard functions and send aid keys (such as PF1) to the host with the click of a mouse. The KeyPad can be represented as either two horizontal or two vertical rows of buttons on a single panel depending on how it is configured. The KeyPad comprises two pads that are toggled through the NextPad button on the pad itself; it can also be displayed with radio buttons for switching between the pads.

KeyPad is sensitive to both the session type and code page, and will display a different pad for 3270, 5250, CICS and VT sessions and for single-byte, double-byte, and bi-directional code pages.

Among its properties is a shape property, which determines whether it takes a vertical or horizontal format. The shape property is an enumeration for which valid values are S2X11 and S11X2.

KeyRemap bean

This visual bean allows users to remap keystrokes to host functions or aid keys. To configure the key mappings, the KeyRemap bean must be displayed and have focus. When a key is pressed, the user is prompted to select a function to which the key stroke will be mapped. Thereafter, the KeyRemap bean intercepts the standard Java KeyEvents, which are fired from the Screen or Terminal bean, and remaps key values that are re-fired as SendKeyEvents back to either the Screen or the Terminal bean.

KeyRemap is sensitive to both the session type and code page, and allows keys to be mapped to different sets of functions for 3270, 5250, CICS, and VT sessions and for single-byte, double-byte, and bi-directional code pages.

Its properties include a sessionType property that affects the set of functions to which keys can be remapped. This property has the same values as the one described above in the section on the Session bean.

FileTransfer bean

This visual bean provides a toolbar interface for transferring files to and from a host. Its properties consist of the default host type and data type. The developer can set these and other properties through its customizer for subsequent modification by the end user.

Macro bean

This non-visual bean records and plays a single macro. It also provides the ability to prompt for user input and extract text from the screen during playback. It must be connected to either a Terminal or a Session bean.

In addition to sending keystrokes, Macro also handles waiting for the host in between key stroke sequences (usually after an aid key). This works in two ways. First, there is a standard wait, whereby Macro will perform a reliable smart-wait that is automatically inserted during recording. These smart-waits take advantage of the Host Access Class Library's screen recognition technology. The second type of wait is a smart wait defined by the user during recording. When the macro is played back, execution will be suspended until the screen described by the user appears. The screen description can be encoded according to the number of fields, number of input fields, and a keyword.

Macro can prompt the user for strings at runtime. When a macro starts, it is scanned for prompt lines; all prompts are presented immediately. Macro can also extract data from the presentation space. During macro recording, the user can specify a rectangular area of the host screen to be extracted. When the macro runs, text in the bounding rectangle is retrieved and loaded into an array of strings. This array is fired in a MacroExtractEvent where any listeners can use the data as they choose. This event is synchronous and does not return until the listener handles it.

Also refer to “More about Macro bean” on page 868.

MacroManager bean

The MacroManager bean can do everything that the Macro bean can do and more. It does not, despite its name, manage Macro beans; it provides a toolbar interface for managing multiple macros. Connected to either a Terminal bean or a Session bean, the MacroManager bean allows you to record, play, load, delete, and edit macros.

You can do simple or advanced recording of a macro. With simple recording, general and reliable screen recognition waits will be inserted automatically into the macro. These screen recognition waits take full advantage of the IBM Host Access Class Library's screen recognition technology.

With advanced recording, you can specifically tailor the screen recognition waits to your host application screens. You can define a screen's characteristics by the number of fields, number of input fields, a keyword, and the operator information area state.

You can also insert prompts into the macro with advanced recording. These prompts can be defined as either password or normal display and automatically place the text that the user inputs into the prompt window during playback. Another feature of advanced recording is inserting extracts into a macro. When the **Extract** button is toggled down, you can mark any part of the presentation space of the Terminal or Session bean you are wired to, and the area marked will be retrieved and fired in an event during playback. A listening bean can capture this data and process it as required.

To manage the persistent storage of macros, you should create an object that implements the MacroIOProvider interface. The MacroIOProvider is responsible for listing all available macros, and saving and retrieving those macros from persistent storage.

If you do not implement MacroIOProvider in your code, MacroManager will go into its default mode of saving and retrieving macros from the home directory in which it was loaded.

Also refer to “More about MacroManager” on page 870.

ColorRemap bean

This visual bean provides an interface for modifying the colors displayed by the Screen or Terminal beans. The host screen consists of fields. The field types are defined by the host type-3270, 5250 or VT. Each field type has its default color. Color remap bean allows the color of a field type to be modified to another color.

When a color is changed through the bean, a ColorRemapEvent is fired to the registered ColorRemapListeners. ColorRemap also listens to ScreenMouseEvents. When a Screen or Terminal bean fires ScreenMouseEvents, ColorRemap automatically displays the correct foreground and background colors for that location.

HostPrintSession

This non-visual bean is an extension of the Session Bean and is used to establish custom print sessions for a host 3270 or a 5250 printer session. It defines the behavior and characteristics of the print session with the host.

This bean provides an extended interface of setter-getter calls to programmatically control the printer device represented by the bean.

HostPrintTerminal

This visual bean is wrapped around the HostPrintSession Bean and is used to establish connection with a host for 3270 and 5250 printer sessions and present the end user with a graphical image that reflects the state of this printer session

Converter

The Converter bean performs a codepage-to-codepage conversion. For the Arabic and Hebrew languages, Converter performs certain BIDI-specific transformations, including the logical-to-visual transform, or vice-versa, and Lam-Alef processing (Arabic only).

The Converter does not use the standard JVM converters. Instead it uses HOD-supplied converters. Here is the list of supported codepages in Table 24-3.

Table 24-3 Converter code pages

Country	Code page
Latin	8859_1, 037, 1046, 1047, 1140, 1146, 1148, 285, 437, 500, 850, 924
Western Europe	1141, 1142, 1143, 1144, 1145, 1147, 1149, 273, 274, 275, 277, 278, 280, 284, 297, 871
Eastern Europe	8859_2, 1153, 852, 870
Arabic	8859_6, 1256, 420, 864
Greek	8859_7, 869, 875
Hebrew	8859_8, 1255, 424, 803, 856, 862
Hindi	1137
Japanese	1390, 1399, 290, 930, 939, 942
Korea	1364, 933, 949
Russian	8859_5, 1025, 1112, 1122, 1123, 1154, 1156, 1157, 1158, 855, 866
Thai	1160, 838, 874
Turkish	8859_9, 1026, 1155, 857
China	1381, 1388, 935
China Taiwan	937, 948, 950, 964, 1371

Two code samples of the Conversion Bean

Example 24-1 Using Conversion Bean

```
package com;

import com.ibm.eNetwork.beans.HOD.Session;
import java.io.*;

public class TestConverter{

    public static com.ibm.eNetwork.beans.HOD.cpc.Converter
          c = new com.ibm.eNetwork.beans.HOD.cpc.Converter();

    public static void main(String[] Args){

      c.init(); //set default attributes

   //set general attributes

   c.setRecordLength(80);
   c.setBinMode(true);

      c.setInputFileName("input.txt");
      c.setInputCodepage("Cp420");
      c.setInputHostType(c.OS390);

      c.setOutputFileName("output.txt");
      c.setOutputCodepage("Cp1256");
      c.setOutputHostType(c.WIN);

   //set BIDI-specific attributes

      c.setInputTextType(Session.VISUAL);
      c.setOutputTextType(Session.LOGICAL);
      c.setInputTextOrientation(Session.LEFT_TO_RIGHT);
      c.setOutputTextOrientation(Session.LEFT_TO_RIGHT);
   c.setSymSwap(false);

   //set Arabic-specific attributes

   c.setNumeralShaping("NOMINAL");
      c.setLamAlef(false);

   //perform the conversion

      c.processConversion();
}
```

Example 24-2 Example of Conversion Bean

```
package com;
import com.ibm.eNetwork.beans.HOD.cpc.*;

import java.awt.*;
import java.io.*;
import java.util.*;
import java.awt.event.*;
import com.ibm.eNetwork.beans.HOD.event.ConvertListener;
import com.ibm.eNetwork.beans.HOD.event.ConvertEvent;
import com.ibm.eNetwork.beans.HOD.Session;

public class TestConverter1 implements java.awt.event.ActionListener
{
  private static Vector ConvertListeners;
  public static ActInfo  currentActInfo;
  public static Converter c;

  public void addConvertListener(ConvertListener l) {
    ConvertListeners.addElement(l);
  }

  public void removeConvertListener(ConvertListener l) {
    ConvertListeners.removeElement(l);
  }


  private void fireConvert(ConvertEvent cevent) {
    if (ConvertListeners != null) {
      Vector l;
      synchronized(this) {
        l = (Vector)ConvertListeners.clone();
      }
      for (int i = l.size() - 1; i >= 0; i--) {
        ((ConvertListener)l.elementAt(i)).execute(cevent);
      }
    }
  }

  public void dispose(){
    ConvertListeners.removeAllElements();
  }

  public void startConversion(){
            ConvertEvent cevent=new ConvertEvent(this, "event ID?",
currentActInfo.toString());
            cevent.setActInfo(currentActInfo);
            fireConvert(cevent);
            return;
  }

  public void actionPerformed(ActionEvent e){
                    System.out.println("Ready for next conversion");
```

```
 }

 public void init(){
   ConvertListeners = new Vector(1,1);
   addConvertListener(c);
   c.addActionListener(this);
 }

 public static void main(String[] Args){

   currentActInfo = new ActInfo();
   c = new Converter();

   currentActInfo.setRecordLength(80);
   currentActInfo.setBinMode(true);

   currentActInfo.setInputPathName("C:"+File.separator+"input.txt");
   currentActInfo.setInputCodepage("Cp420");
   currentActInfo.setInputHostType(c.OS390);

   currentActInfo.setOutputPathName("C:"+File.separator+"output.txt");
   currentActInfo.setOutputCodepage("Cp1256");
   currentActInfo.setOutputHostType(c.WIN);

  //set BIDI-specific attributes

   currentActInfo.setInputTextType(true);
   currentActInfo.setOutputTextType(false);
   currentActInfo.setInputTextOrient(true);
   currentActInfo.setOutputTextOrient(true);
   currentActInfo.setSymSwap(false);

  //set Arabic-specific attributes

   currentActInfo.setNumeralShaping("NOMINAL");
   currentActInfo.setLamAlef(false);

   TestConverter1 theTest = new TestConverter1();
   theTest.init();
   theTest.startConversion();

 }
}
```

24.5.2 Automated host navigation

Please read 24.4.3, “Automated host navigation” on page 855 as an introduction to conceptions of screen recognition.

More about Macro bean

The Macro bean in the Host Access Beans for Java API is another assistive technology. Macro is a non-visible component, although it is typically used in a GUI application. The Macro bean serves as a tool for the developer (or application at runtime) to define a macro or a script to navigate host screens.

Macro is a scripting-oriented abstraction of the screen recognition technology. The user creates an XML-based script to define screens and the actions associated with those screens. A macro script used by the Macro bean contains three elements:

A screen description The criteria used to identify a unique screen or screen state.

Actions to take What to do when the screen is recognized.

Next screen (optional) A pointer to the next screen definition depending on the result of actions on the current screen.

Scripts are interchangeably executable on the general-purpose scripting engine. The engine can be extended and enhanced, while maintaining backward compatibility to older script syntax. Alternative scripts can be deployed according to scripting engine capabilities. Macro scripts can be serialized or loaded from a text file. A provider interface is available to insulate the scripting engine from the storage or transport mechanism used to load/store macro scripts.

Macro bean uses XML for scripting because a macro is better suited to the state machine model (the main reason for the move: XML is tailor made for a state machine).

The idea of a state machine may be fairly new to you. The idea behind a state machine, especially in the Macro bean context, is simple. Think of how you use a host system from a terminal or a terminal emulator (like Host On-Demand). The process you follow when you interact with a host system is illustrated in these steps:

1. The host sends an expected screen down to you at your terminal.
2. You look at and understand which screen is presented to you.
3. You take the required actions based on your understanding (type keystrokes, and so forth).
4. Another screen is presented after these actions.
5. If you see the screen you expected, repeat steps 2, 3, and 4.
6. If you do not see the screen you expected, call the help desk or handle the error.

This is the idea behind a state machine in the Macro context (although the Macro cannot call the help desk for you). The states are the screens you expect to see, and you take actions on those screens to change from one state, or screen, to another. That is it: see a screen, perform the action, see the next screen. It is easier to understand (and program) a macro with this approach than having several if-then-else and do-while programming statements. Remember: see a screen, perform the action, see the next screen.

The following are valid Macro elements. The tag names are suggestive of their function.

Example 24-3 Macro elements

```
<HAScript>
  <vars>
     <create>
  <screen>
     <comment>
     <description>
         <oia>
         <cursor>
         <numfields>
         <numinputfields>
         <string>
         <attrib>
         <customreco>
         <varupdate>
  <actions>
         <prompt>
         <input>
         <extract>
         <message>
         <trace>
         <filexfer>
         <pause>
         <mouseclick>
         <boxselection>
         <commwait>
         <custom>
         <varupdate>
         <playmacro>
         <if>
         <else>
         <runprogram>
  <nextscreens>
         <nextscreen>
  <recolimit>
```

These XML elements and their attributes are valid in the Host On-Demand Macro XML namespace. This description of the elements is structured like an actual macro file. Element and attribute values are not case sensitive.

More about MacroManager

MacroManager provides an end-user convenient toolbar when it makes sense to let the user load a macro script appropriate to the situation from a library. MacroManager must have an associated Macro bean. The API allows that association to be set in different ways.

MacroManager on the Host On-Demand toolbar is an excellent way to record macro scripts for using in custom applications programmed with HABJ. There is an excellent designer-editor customer window associated with MacroManager.

Please see Appendix C, “An example of MacroIOProvider” on page 1059 for a demonstration of MacroManager in action in the context of Host On-Demand client.

HOD V8 versus PCOMM Macro

The HACLJ and HABJ Java code level of Personal Communications is at the level of Host On-Demand 4.0. Host On-Demand 8.0 contains improvements and extensions in the Macro bean. If you made a strict comparison, the differences might present incompatibilities: all of Personal Communications code compiles using the Host On-Demand 8.0 JARs, but the reverse is not true. HOD V8.0 has extensions and features not found in Personal Communications Macro support.

Personal Communications desktop emulator has a macro facility available on its toolbar. The underlying mechanism and scripting languages bear no relation to the Host On-Demand-descendant Java Macro bean.

24.6 Java 2

Since the release of Java Runtime Environment 1.1.8, Sun has introduced several new technologies and methodologies that should be addressed to ensure a properly designed, implemented, and executed applet or application. IBM urges all developers to use the latest available Java 2 Plug-in for any technologies that were added after the JRE 1.1.8 specification.

The Host Access Beans for Java now supplied as separate library sets targeted for JDK1.1.8 or Java2 (JDK 1.4.0). The debug and release libraries are installed in these directories:

<install dir>\toolkit\jars\jdk1.1

<install dir>\toolkit\jars\java2

The files supplied include a `2` suffix when the files are unique for Java 2. For instance, habasen.jar is for jdk1.1 and habasen2.jar is for Java2

The Java 2 JAR libraries can only be run in a browser that has the Java 2 plug-in enabled or launched in a Java 2 virtual machine. The Java 2 version is Swing-based and should integrate well with other Swing components. There are known issues when building applications or applets that use both AWT components and Swing components. For more information on compatibility between AWT and Swing components, see the Sun Java Web site:
http://www.java.sun.com

The Java 2 version of the Host Access Beans offers accessibility, autoIME/on the spot conversion for double-byte character set (DBCS) languages, and print screen enhancements. Pure JDK 1.1 applets and applications that use the Host Access Toolkit JDK 1.1.8 libraries are runtime compatible with the Java 2 Virtual Machine. However, applets and applications built with the Java 2 libraries are strictly incompatible with a JVM version 1.1.

The traditional JDK1.1.8 version of our APIs is most suited for applets intended for JDK1.1-based browsers or for applications launched into a Java Virtual Machine version 1.1. These JDK1.1.8 libraries (JAR and CAB) are compatible with previous versions of the Host Access Toolkit.

24.6.1 Security

Note: Java security is an evolving area. The security model has become more “granular.” Some browser implementers took an individual proprietary path. Vocabulary usage has been inconsistent. You, the end user, will have to develop a mental picture that rationalizes all of the apparent confusion.

The classes of the HACLJ and HABJ API libraries were written to be compatible with the native security mechanisms of the two main popular Web browsers: Microsoft Internet Explorer and Netscape Navigator. Those two are JDK 1.1-based. The libraries have subsequently been updated to operate in the Sun Java 2 1.4.x Plug-in environment.

Netscape uses its proprietary netscape.security package. Internet Explorer uses its proprietary com.ms.security package. Sun Java 2 is based on the java.security package. Each is unrelated to the others. Therefore, the library code (and by implication, your code) must be written to accommodate usage in various browser and security environments. The coding of the Toolkit libraries specifically distinguishes between Netscape, Internet Explorer, and “other.” The “other” implies Java 2.

A library that has been signed digitally may also be “granted” permissions. The “release” versions of the Toolkit libraries have been signed with IBM's certificate and granted “AllPermissions.” Your digitally signed custom libraries should grant the level of permission(s) appropriate to your purpose

A “trusted” action is an operation or external access that is prohibited by default. The requestor is not trusted to perform it, by default. Permission (Internet Explorer) or privilege (Netscape) must be asserted (Internet Explorer) or enabled (Netscape) in order to overcome the default prohibition.

The installed security manager will allow certain prohibited-by-default trusted actions to succeed provided that all of these conditions are met:

1. That the executing code was loaded from a library
    a. That it was digitally signed by a trusted certificate
    b. And that the library was granted sufficient permissions
2. That the executing scope has already asserted enabled the appropriate specific permissions or privileges

At certain places in the HACLJ and HABJ code, trusted actions are taken in a certain scope of execution. Prior to that action and within that same execution scope, appropriate privileges must be enabled. The policy rules of the security manager of the Java Virtual Machine determine what constitutes a trusted action. Scope of execution means that an enabled privilege remains in effect for the duration of the enclosing method call and its sub-method calls; privilege ends when the enclosing method returns, or when the privilege is disabled, whichever occurs first.

If your application code must perform a trusted action, you must code the necessary privilege enablement. In certain situations, a trusted action might originate as a call to a public method in the API library. It must be preceded by the appropriate privilege enablement, which is determined by experimentation.

In the subsequent discussion, the example trusted action is an instance of an applet class creating or truncating a file on the local hard drive and writing to it. Normally the “sandbox” created by the browser security manager prevents that action (it is a “trusted” action). Therefore, your code must specifically enable the appropriate privilege, the security manager must agree that the privilege is the correct one, and the security policy in force must allow that privilege to be enabled in the runtime code. Additionally, your code must load from a digitally signed library that has been granted sufficient permissions. If any of these conditions are not met, then the trusted action will fail with a characteristic exception being thrown.

“Digital signing”, or “code signing”, is the practice of placing an unalterable, authentication “stamp” on a code library. This stamp asserts that the encompassed library is actually developed by a particular organization. To the extent a user trusts the organization, the end user will trust the library and allow all requested instructions to occur. Java supports this security model because it guards against running malicious code (such as inappropriately erasing files) provided by organizations and entities unfamiliar or untrusted to the user. To sign code, one must obtain an authentic certificate from a Certificate Authority such as Thawte Consulting or VeriSign, Inc. These certificates are recognized by the browser or plug-in and are presented to the user for approval or rejection of the requested privileges.

The security manager

Internet Explorer running with the Microsoft Java Virtual Machine installs its own security manager. Likewise, Navigator installs its own security manager. When appletviewer.exe is run, it installs its own security manager, which cannot be disabled. Usually when an application is started from the command line, there is no security manager installed by the virtual machine. Under Java 2, there is a command-line flag for java.exe, `-Djava.security.manager`, which signals the virtual machine to install the Sun Java 2 security manager before executing code.

When a JVM does not have a security manager installed, all trusted actions are automatically enabled. Failure of a trusted action, if it occurs, will be on the merits and not on “permissivity.” This mode is equivalent to a superuser. It is an excellent mode for code logic and flow development, but unsuited to deployment of a mission-critical application. The implementation for the application design will require identification of all trusted actions and accommodation to the security policy of the deployed application.

Netscape 4.7

When Navigator loads and executes an applet class, it searches the libraries named in the ARCHIVE parameter of the APPLET tag and searches for “loose classes” (see “Effect of “loose classes”” on page 881) in the folder where the HTML file is located. A packaged library may be a JAR or a ZIP file. The JAR file may, or may not, be digitally signed.

When code execution arrives at:

```
<PrivilegeManager>.enablePrivilege("<a NS privilege string>");
```

the Navigator security manager will check whether that path-and-distinguished-name-specific class is known to the browser. If it is not known, Navigator will display a window to inform the user of a needed decision. If the user makes a "grant" decision, that is policy momentarily stored by the browser. The user may also mark that policy decision as "remember."

The specific policy decision is stored in a browser database entry in the form of a pair of strings representing "key" and "value". For a trusted, digitally signed JAR, the key is the trusted certificate and the value is the specific privilege. For an unsigned library, the key is the URL of the library and the value is the specific privilege. Normally, an entry in the database lasts only as long as the browser session. A "remembered" entry persists across browser sessions.

Internet Explorer

When Internet Explorer loads and executes an applet class, it searches the libraries named in the “cabinets” PARAM tag within the scope of the APPLET tag. The library format is CAB, which is created by the Microsoft cabarc.exe tool. The CAB may be signed with the signcode.exe tool.

When code execution arrives at:

```
PolicyEngine.assertPermission(PermissionID.<permission mnemonic>);
```

Internet Explorer does not offer the user an opportunity to decide policy. If the CAB library is not digitally signed by a trusted certificate, the assertion is denied and the subsequent trusted action fails with a characteristic exception thrown.

Normally Internet Explorer does not use JAR or ZIP files, unless they are path-specifically mentioned in this Windows Registry entry:

```
HKLM\Software\Microsoft\Java VM\TrustedClasspath
```

That entry is a global CLASSPATH and the enumerated JARs, ZIPs and class files are granted all permissions (superuser). A CAB file, signed or unsigned, named in that Registry entry is disregarded by the IE security manager.

Java 2 Plug-in

The Java 2 security manager responds to two policy files. See Sun's documentation at:

http://java.sun.com/docs/books/tutorial/security1.2/summary/tools.html

We are interested in a user's “.java.policy”, which is the target of the Java 2 policytool.exe. The installation of the Plug-in JRE does not normally install .java.policy.

The purpose of the .java.policy file is to express the baseline permissions of the virtual machine sandbox whenever the Java 2 virtual machine is called into action for that logged in user. The Java 2 Plug-in can be parameterized (on Windows) to be the default JVM for Netscape and for Internet Explorer 5.+.

When a trusted action call is made, the Java 2 security manager relies on the permissions in the.java.policy file. If there is no.java.policy file, the programmer may have used Java 2 syntax to assert a permission. Absent that, the Java 2 security manager displays a window to inform the user of the permission request and asks for a GRANT type reply. This happens only once on the first encounter to a trusted action. GRANT can last just for the Plug-in session or “always.” All trusted actions are covered by this GRANT action. An approved GRANT, which was indicated to the browser as one to remember, can be revoked by removing the mentioned certificate copy from the Java 2 Plug-in properties window in the Services folder.

Additional information about Java 2 security

We recommend two books dealing with Java 2 security:

- *Java 2 Network Security* by M. Pistoia et al., June 1999, IBM Form Number: SG24-2109-01, ISBN: 0-130-15592-6, covers many topics of interest to Java programmers dealing with the practicalities of security programming and digital signing. It was written when the Java 2 security API was in its formative stage.
- *Java Security: 2nd Edition* by Scott Oaks, May 2001, O'Reilly & Associates, Inc. ISBN: 0-596-00157-6, is an exhaustive presentation of the Java 2 security model and associated Java technologies.

24.6.2 Permissions programming examples

The sample code shown in Example 24-4 illustrates alternative permissions codings. Example 24-5 shows a sample HTML page to execute the applet shown in Example 24-4.

Example 24-4 Permissions programming example

```
package trustedaction;
import java.awt.*;
import java.awt.event.*;
import java.applet.*;
import java.io.*;
import netscape.security.*;
import com.ms.security.*;
import com.ibm.eNetwork.HOD.common.*;  // Obtain Environment.class for
detecting the browser

/**
 * AS-IS sample : not intended as example of best Java practices
 *
 * To compile, use \HostOnDemand\HOD\hoddbg.jar, java40.jar from NS 4.7 and
com.ms.security.*
 */
public class TrustedActionApplet extends Applet {
        // borrowed from HOD: capable of detecting browser
  Environment env = Environment.createEnvironment();
  boolean isStandalone = false;
  /**Get a parameter value*/
  public String getParameter(String key, String def) {
    return isStandalone ? System.getProperty(key, def) :
      (getParameter(key) != null ? getParameter(key) : def);
  }
  /**Construct the applet*/
  public TrustedActionApplet() {
  }
  /**Initialize the applet*/
  public void init() {
    try {
      jbInit();
    }
    catch(Exception e) {
      e.printStackTrace();
    }
  }
  /**Component initialization*/
  private void jbInit() throws Exception {
      this.setBackground(Color.red);
      // is it Internet Explorer?
      if
(Environment.getUseSecurityManager().equals(Environment.SECURITY_MGR_IE)) {
          System.out.println("Detected IE");
          jbInit_IE();
      }
      else  //is it Netscape?
      if
(Environment.getUseSecurityManager().equals(Environment.SECURITY_MGR_NS)) {
          System.out.println("Detected NS");
          jbInit_NS();
      }
      else {  // will assume that it is Java2 PlugIn
      System.out.println("Fell through to OTHER");
      openFile();
      }
  }
        // Internet Explorer proprietary PolicyEngine and Permission.ID
  private void jbInit_IE() throws Exception {
      System.out.println("ATTEMPTING:
PolicyEngine.assertPermission(PermissionID.FILEIO)");
```

```
      PolicyEngine.assertPermission(PermissionID.FILEIO);
      System.out.println("SUCCEED:
PolicyEngine.assertPermission(PermissionID.FILEIO)");
      openFile();
  }
        // Netscape 4.+ proprietary PrivilegeManger and privilege string
  private void jbInit_NS() throws Exception {
      System.out.println("ATTEMPTING:
<PrivilegeManager>.enablePrivilege(UniversalFileWrite)");
      netscape.security.PrivilegeManager pm = new PrivilegeManager();
      pm.enablePrivilege("UniversalFileWrite");
      System.out.println("SUCCEED:
<PrivilegeManager>.enablePrivilege(UniversalFileWrite)");
      openFile();
  }
        // Assuming that Java2 PlugIn and .java.policy file controls
  private void openFile() throws Exception {
      System.out.println( "OPEN FILE");
      FileOutputStream fos = new FileOutputStream("c:\\F020117.txt");
      PrintStream prtS = new PrintStream(fos);
      prtS.println( "The TIME=" + System.currentTimeMillis());
      fos.close();
      prtS = null;
      fos= null;
  }

  /**Start the applet*/
  public void start() {
  }
  /**Stop the applet*/
  public void stop() {
  }
  /**Destroy the applet*/
  public void destroy() {
  }
  /**Get Applet information*/
  public String getAppletInfo() {
    return "Applet Information";
  }
  /**Get parameter info*/
  public String[][] getParameterInfo() {
    return null;
  }
```

Example 24-5 Sample HTML page

```
<HTML>
<HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=windows-1252">
<TITLE>
HTML Test Page
</TITLE>
</HEAD>
<BODY>
```

```
trustedaction.TrustedActionApplet will appear below in a Java enabled
browser.<BR>
<APPLET
  ARCHIVE  = "hoddbg.jar,appletCode.jar"
  CODEBASE = "."
  CODE     = "trustedaction.TrustedActionApplet.class"
  NAME     = "TestApplet"
  WIDTH    = 400
  HEIGHT   = 300
  HSPACE   = 0
  VSPACE   = 0
  ALIGN    = middle
>
<PARAM NAME="cabinets" VALUE="hoddbg.cab,appletCode.cab">
</APPLET>
</BODY>
</HTML>
```

Example 24-6 shows how to compile the example.

Example 24-6 Compile the example

```
SET JDK=%ibmjdk1%
%JDK%\bin\javac -d . -classpath
hoddbg.jar;.\PolicyEngine;.\PrivilegeManager\java40.jar;%JDK%\lib\classes.zip;.
trustedaction\TrustedActionApplet.java
```

24.6.3 Debugging runtime failures

This section discusses how to distinguish between security exceptions and programming bugs as the cause of runtime failures.

Messages sent to the Java console are an important source of information in developing and debugging Java applets and applications. When the program execution is started from a command-line window, that window usually serves as the Java console display area. For applets running in a browser, there is a menu bar option to display the Java console associated with the browser's native Java Virtual Machine (JVM). In the case of a browser employing the Sun Java 2 Plug-in, the Java console is accessed through the runtime icon for the JVM. In other words, when an applet is loaded, the browser first loads the Plug-in before starting the applet. Usually an icon appears in the desktop system tray to represent the Plug-in process. That icon gives menu access to the Java console.

Java methods are often designed to throw an exception for error conditions. The try-catch control block is used to catch exceptions at strategic points for the purpose of recovering from an error or to exit gracefully. Try-catch blocks are important debugging points where the “printStackTrace” method can be called. A stack trace can be obtained at any point with a “Thread.dumpStacktrace();” statement.

When a “trusted” action is performed, it will succeed provided the proper permission is in effect and the security manager concurs. An exception will be thrown by the security manager (if it is installed) when a “trusted” action is attempted without sufficient permission(s).

Suppose you have developed an applet in such a manner that it can also be run as a stand-alone application (it has a “main(...)” entry point). A puzzling situation arises. When the application is run from the command line, everything works as expected. In contrast, when that same applet is run in a browser through an HTML file, there are exceptions being reported on the Java console. In the case of a HACLJ or HABJ applet, a connection to the target host cannot be established. The exceptions all seem to originate deep in the code of the HACLJ/HABJ classes. Are these unexpected bugs in the API library?

If this failure is due to insufficient or incorrect permissions exerted, they will disappear when the applet is run in a “superuser” mode. If these are determinate bugs in the library, then even in superuser mode they will persist.

Under the Java 2 security model

AllPermissions, in the Java 2 Security model, is the equivalent of a superuser. Any trusted action is permitted always. Therefore, if your applet in a browser were to run as a superuser, only bugs would be the source of exceptions. It is simple to create the superuser mode under Java 2.

Under the Java 2 Security model, JVMs are traditionally configured with a java.policy file. This file identifies which permissions a class, be it an applet or application, may obtain from the JVM. All Java 2 SDKs contain a `policytool.exe` to modify these settings. See the Sun document at:

http://java.sun.com/docs/books/tutorial/security1.2/summary/tools.html

For example, if you wanted to effectively turn off security for all classes on the C drive, you would:

- Launch (JRE)\bin\policytool.exe. If a window appears stating that the .java.policy file cannot be found, write down the location it attempted to read from.
- Click **Add Policy Entry**. Specify the codebase as file:/C:/- (Note the required type of slash even for Windows.)

- Click **Add Permission**. From the Permission pull-down, select **AllPermission**. Click **OK** to close both windows.
- Save the file. If creating a new file, use the location specified when you first opened policytool.exe.

For all JVMs that use this policy file, “all permissions” (superuser privilege) will be granted to any class located on the C drive. This mechanism works identically for Netscape and Internet Explorer when Sun's 1.3.1 Plug-in supplies the JVM.

Under the Internet Explorer TrustedClassPath model

The Windows Registry entry `HKLM\Software\Microsoft\Java VM\TrustedClasspath` can be very helpful in quickly creating a “superuser” mode. Any fully qualified JAR or ZIP file path name in that entry is:

1. A global CLASSPATH library, and
2. Granted all-permissions for any trusted action performed by code in that library

Typically an HTML file for Internet Explorer will have the following line:

```
<PARAM NAME="cabinets" VALUE="<list of CAB files>"
```

Remove that line. As a further simplification, remove these typical lines:

```
     CODEBASE = "."
     ARCHIVES = "<list of JAR and ZIP file>"
```

Next, use **`Regedit`** to modify the Windows Registry (carefully). In the key `HKLM\Software\Microsoft\Java VM\TrustedClasspath`, write a semi-colon separated list of full path names to all needed JARs and ZIP file.

The use of CAB files in an Internet Explorer context includes, but goes beyond packaging Java classes. This is an entry point Microsoft Knowledge Base Web page to cover the entire topic:

HOWTO: Make Your Java Code Trusted in Internet Explorer

http://support.microsoft.com/default.aspx?scid=KB;EN-US;q193877&

Under LINUX

Netscape V7 with a Java 2 Plug-in is available for Linux; therefore, the appropriate information in “Under the Java 2 security model” on page 879 applies here.

Effect of “loose classes”

We define “loose classes” as a folder hierarchy of classes partially duplicating the content of digitally signed JAR libraries. Suppose the JVM searches the loose classes first and then the signed JAR libraries. In an extended search for members of a given package, it may report (typically) a NullPointerException or ClassDefNotFound exception. The underlying reason would be that members of the same package are located in two “libraries” that do not have the same digital signature. Loose classes cannot be signed; therefore their “signature” is different. Consolidation and unified signing is the solution.

Remember that these loose classes themselves have no digital signature and no assigned level of “permissions granted.” If one of those classes attempts a “trusted” call, even if the code exert a “permission;” it will fail with a security exception.

Environmental CLASSPATH failures

Some development environments and installed applications set the local user or global environmental CLASSPATH variable. Suppose that your application launch command also enumerates the %CLASSPATH% environmental variable. When you attempt to run your application in a local hard drive, the JVM may inadvertently be searching duplicate but different versioned package libraries. That may cause unexpected runtime failures or component misbehaviors.

24.7 Host On-Demand EHLLAPI Bridge

The IBM EHLLAPI Enablemant Tool V2.0 (previously IBM Host On-Demand EHLLAPI Bridge) is a technology that allows an application written using a variety of HLLAPI-based languages to use Host On-Demand as the target emulator. There is a large base of existing EHLLAPI code developed before the advent of Java and Host On-Demand. Much new EHLLAPI code is being developed. The benefit of the EHLLAPI Bridge is that client applications can readily migrate from one emulator, such as Personal Communications or Attachmate, to Host On-Demand. Sometimes the original EHLLAPI binary can be used directly, if no minor code adjustments are needed for Host On-Demand compatibility. This technology is not shipped with either Host On-Demand or the Host Access Toolkit. The packaged file, `ehllapi.exe`, can be downloaded by registered users free of charge from the following Web site:

http://www.ibm.com/software/webservers/hostondemand/downloads.html

24.7.1 Operational configuration

The typical EHLLAPI custom application is written in a Win32 API-based programming language for the Windows operating system, such as C/C++ or Visual Basic or REXX. The application is used in conjunction with one or more emulator sessions running on the desktop. The EHLLAPI program communicates with the emulator program through Windows and OS/2 compatible DLLs. The emulator window opens and maintains a session with the target host. The stand-alone EHLLAPI program uses a set of EHLLAPI API functionalities to interact with the host terminal program presented in the emulator session window. EHLLAPI API programming is discussed in detail with code examples in the *Emulator Programming* document (pcep.pdf), available in the companion Personal Communications V5.6 product.

24.7.2 Supported interfaces

These are the supported interfaces:

- Industry Standard EHLLAPI 16-bit
- Industry Standard EHLLAPI 32-bit
- IBM Enhanced EHLLAPI 32-bit
- WinHLLAPI 16-bit
- WinHLLAPI 32-bit
- DOS HLLAPI

24.7.3 Supported non-standard interfaces

- IBM Personal Communications PCSAPI Interface
- Attachmate Corporation EAL
- IBM Host On-Demand Utility Bridge

24.7.4 Supported Platforms and JVM environments

The platforms supported are:

- Windows 98
- Windows Me
- Windows NT (at least SP5 and preferably SP6a)
- Windows 2000 (preferably with the latest Service Pack)
- Windows XP

The EHLLAPI Bridge runs on Host On-Demand versions 4.0 or later. The PCSAPI support the Extensions for migrating Attachmate Corporal EAL require Host On-Demand versions 6.05c, 7.02, 8.0, or later.

If the HLLAPIEnabler Applet fails to load and the Java console shows an error saying `RNIGetCompatibleVersion not found`, this means the user does not have the appropriate level of the Microsoft VM. For most MS VM updates please visit:

http://windowsupdate.microsoft.com

As of this writing there is a special situation for users of Internet Explorer on Windows XP. The details are presented here:

http://www.microsoft.com/java/xp.htm

24.7.5 Installation

Provision is made for running existing code written for Windows and also written for the earlier DOS environment.

Attention: Previous Users of the Utility Bridge SDK and Utility Bridge Macro Conversion Tool:

This installation will uninstall all previous bridge versions. If you have macros that have been converted with the previous tools, they will no longer run after installing this. Please refer to the *EHLLAPI Bridge Readme* for instructions on how to avoid conflicts with this upgrade. A more compatible version of the Macro Conversion and Runtime will be provided at a later date.

Windows installation

To automatically install the EHLLAPI enablement software on a Windows workstation using InstallShield, you must log in as administrator, or a user that is a member of the administrators group before you can install the EHLLAPI Bridge on your computer. Locate the `Ehllapi.exe` installer file that was downloaded from the Web page mentioned above. Double-click the icon and choose all default values during the installation process, unless a different installation location is desired. Restarting your computer is necessary, except for Windows 2000 and Windows XP.

Upon restart the PATH variable value may be similar to this example from Windows 2000. Notice that the system search path finds the EHLLAPI Bridge folder first.

For PCSAPI and Attachmate EAL support, you must use the Host On-Demand Deployment Wizard to set parameters in the HTML file. The parameter to set is `ENABLE_PCSAPI=YES`, which can be set as a HTML parameter.

Tip: Check the content of the System PATH environmental variable. In the case of the default installation location, "`C:\Program Files\IBM\EHLLAPI;`" should precede the path location of any other Win32API-based emulator product, such as Personal Communications. The reason is that the DLLs installed for EHLLAPI Bridge have the same standard names as the DLLs of EHLLAPI-capable emulator products. For this bridge to work in conjunction with Host On-Demand, the Windows operating system must discover the EHLLAPI Bridge DLLs before those of the other emulator product. Consequently, if you try to use that other emulator product, it will likely fail with an unexpected error: the Windows system has located the “incorrect DLLs.” The implication is that deployment of Host On-Demand EHLLAPI Bridge may require the removal of other Win32API-based emulator products so as to avoid “DLL confusion”

Configure a Host On-Demand emulator icon. In the Properties window for any sessions to be used with EHLLAPI applications, do the following on the Advanced tab:

- Set the Auto-start pull-down to Applet.
- Type in the Auto-Start Name Field this class name: `com.ibm.eNetwork.hllbridge.HLLAPIEnabler.`
- Alternatively, you may run this applet after the session has been started by clicking **Assist --> Run applet** from the session menu bar.

DOS installation

The EHLLAPI Bridge can be used to run DOS EHLLAPI programs but it requires some additional setup. The following assumes the default installation location of the EHLLAPI Bridge:

C:\Program Files\IBM\EHLLAPI

Windows NT

To Enable DOS EHLLAPI Programs on Microsoft Windows NT:

- The additional binary files are located in:

  `C:\Program Files\IBM\EHLLAPI\DOSHLLAPI\NT.`
- Place the file HLLDRVR.SYS in your “windows directory”\System32\Drivers subdirectory.
- Place the file HLLVDD.DLL in the same directory as the rest of your HLLAPI Bridge DLLs.

- In the subdirectory “windows directory”\System32 is a file called Config.NT. Modify this file by placing the following line at the end:

```
device="windows directory"\System32\Drivers\HLLDRVR.SYS
```

- Restart your computer.

The bridge will now work without any further special actions.

Windows 9x

To Enable DOS EHLLAPI Programs on Microsoft Windows 95 or Microsoft Windows 98:

- The additional binary files are located in:

  C:\Program Files\IBM\EHLLAPI\DOSHLLAPI\Win9x.

- Place the file DOSHLL.VXD in your "windows directory"\System subdirectory.
- Place the file DOSHLL.EXE in the same directory as the rest of your HLLAPI Bridge DLLs, such as C:\Program Files\IBM\EHLLAPI.
- In the "windows directory" is a file called System.INI. Modify this file by placing the following line at the end of the section headed by "[386Enh]":

```
device="windows directory"\System\doshll.vxd
```

- Restart Windows.

To use the bridge for DOS EHLLAPI programs, start the program DOSHLL.EXE and then run your program.

24.7.6 Operation

First start one or more properly configured Host On-Demand emulator sessions. Then start the EHLLAPI application. The EHLLAPI program should run normally and expected host actions should occur in the Host On-Demand emulator window.

Known limitations

The EHLLAPI Bridge is an evolving tool with certain known limitations:

- Structured Fields, related functions (120-127) are not supported.
- WinHLLAPI Extensions for Asynchronous calls and blocking functions are not supported.
- LockPS(60)/LockWindowServices(61) are not supported (used when multiple apps are connected to the same session).
- StorageManager(17) is supported for WinHLLAPI only.

If any of the above unsupported options are used by the invoking application, a message window will be displayed notifying the user that the application may not work as expected.

Additionally, the following restrictions apply:

- SendFile(90)/ReceiveFile(91) - not supported for 5250 sessions.
- SetSessionParms(9) EAD/NOEAD,SO/NOSO/SPACESO - these DBCS-only parameters are not supported.
- EXTENDPS/NOEXTENDPS (5250 only) - CopyPS, CopyPSToString, CopyStringToPS, CopyStringToField, CopyFieldToString, and SearchField - will always return any messages on line 24 (like EXTEND_PS), but will never return a 25th line (such as NOEXTEND_PS).
- SUPER_WRITE, WRITE_SUPER, WRITE_WRITE, WRITE_READ, WRITE_NONE, READ_WRITE - these parameters will be ignored; standard EHLLAPI supports only one application connection to a session at a time.
- NOBLANK - this parameter will be ignored, standard EHLLAPI default of BLANK will always be used.
- KEY$xxxx - this parameter will be ignored, standard EHLLAPI default of NOKEY will always be used.
- Prior to the loading and availability of Host On-Demand 4.0 CSD 1, closing a Host On-Demand session with the X button in the upper right-hand corner of the Host On-Demand Session Frame can have the side effect of requiring a Browser restart.
- To support CICS and VT gateways, it will be necessary to obtain and load Host On-Demand 4.0 CSD 1 or later. Prior to the availability and loading of this level of code, using the CICS or VT gateways (Icon Types) will abort the Bridge enablement. CICS users can use a 3270 connection to a CICS session and everything will work appropriately.
- REXX support is required for starting and stopping sessions using PCSAPI32.dll.

Attachmate EAL support

Depending on how your program uses the EAL Library, it might be necessary to make conversions to your program to use these extensions. In addition, some behaviors might differ from the original implementation.

EAL programs must link with ATMAPI32.DLL to run. This linkage can be done through the compiler (implicit linkage), or by specific code (explicit linkage). Programs written with C, C++, or a similar language and link with the import library ATMAPI32.LIB use implicit linkage. Code written using higher level languages such as Microsoft Visual Basic or Borland Delphi, or C/C++ code that use the Win32 SDK calls to LoadLibrary() and GetProcAddress() link explicitly. The major difference is that implicitly linked code does not require the APIs to have the same names, but explicitly linked programs do. This affects how this product is used.

- If your program has been linked implicitly, by using the EAL API directly and by linking with ATMAPI32.LIB, then your program should run as is and unmodified, assuming that behavioral differences do not affect your logic.
- If your program is linked explicitly, then some modifications will be necessary, which can be achieved by a simple text replace operation.

If the source for your program is available, then it would be best to convert it to the new APIs regardless of linkage.

Tracing

There is tracing that is specific to the EAL extension code. To enable tracing, you must set the environment variable `UTL_DEBUG=YES`. This causes the Bridge to log all function calls and parameters to utlTrace.log, which is saved in the same directory as the application.

To set the environment variable:

1. On the Windows desktop, right-click **My Computer** and select **Properties**.
2. On the Advanced tab, click **Environment Variables**.
3. Under System variables, click **New**.
4. In the New System Variable window, type `UTL_DEBUG` in the Variable Name field.
5. In the Variable Value field, type `YES`.
6. Click **OK**.

The log file is a continuous record, so be sure to delete the environment variable when done tracing. The log file has a maximum file size of 16 MB. After this size has been reached, the log wraps to the beginning and starts overwriting older data.

Conversion process

To make the conversion from Attachmate to Host On-Demand, you must first understand that there are some fundamental differences between the two products. Host On-Demand is a Java-based product that runs in a protected framework. The Java Virtual Machine is the functional equivalent to a different computer, so information from your native operating system is usually unavailable to Java programs. This bridge is designed to get around those obstacles, but you must take certain steps. Further, functional differences between the products limit full migration for some programs, though most convert well.

Session Letters for Attachmate are used only for EHLLAPI compatibility, so configurations must be separately assigned to those letters. To this end, a settings utility is provided to make these assignments. This utility must be used to define session letter assignments and to dictate which program and URL will be used to start Host On-Demand, or UTLStartSession, UTLGetSessions, and UTLListSessions will not function properly.

If the source code for your program is available, then it will be possible to convert your code to use this implementation by simply using a text replace operation to find the old APIs and constants by replacing instances of the pattern ATM with the pattern UTL. This should be done for function names and constants, but not for DLL, LIB, or other file name references. If you use the LIB file, you can continue to use the existing one.

If you use Visual Basic, then you must include the file atmapi32.bas as part of your project. This install provides a similar file that replaces the original file, but certain unsupported constants are missing. If you use those constants or if you are unsure, it might be best to modify your existing version of this file. Likewise, you must convert any other language, such as Delphi or PowerBuilder. For example:

ATM_constant becomes *UTL_constant*

ATMfunction becomes *UTLfunction* Also, you should replace any references to the product name, `Extra`, with five underscores (_____).

We recommend that you modify the constants first and take caution not to alter coincidental pattern matches within your code. No additional changes should be necessary unless behavioral differences need to be accounted for.

If the source code is not available, then it is still possible to make the conversion for explicitly linked programs. You can use BinaryUpdater, a program provided with this product, to safely change the function names within the compiled program.

Known behavioral differences

Several Functions exist that are either exclusive to the Competitor product, or are impractical to implement at this time. Also, there are certain parameters that are product exclusive, so those parameters will have default defined behavior. All functions are recognized, but un-implemented functions will always return UTL_SUCCESS. The following enumerates known differences in behavior and limitations:

Functions incompatible with Host On-Demand:

- AllowUpdate - Allows the emulator to paint the PS in response to a host update after a BlockUpdate call has been made
- BlockUpdate - Prevents the emulator from painting the PS in response to a host update
- HoldHost - Supposedly prevents the Host from updating
- ResumeHost - Allows host updates after a HoldHost call has been made

Unsupported Attachmate-specific calls:

- UTLGetEmulatorPath - always returns UTL_SUCCESS.
- UTLGetLayoutName - always returns UTL_SUCCESS.
- UTLOpenConfiguration - always returns UTL_SUCCESS.
- UTLCloseConfiguration - always returns UTL_SUCCESS.
- UTLOpenLayout - always returns UTL_SUCCESS.
- UTLExecute - always returns UTL_SUCCESS.
- UTLRun_____Macro - always returns UTL_SUCCESS.
- UTLRun_____MacroAsync - always returns UTL_SUCCESS.
- UTLGetError, UTLShowLastError - always returns UTL_SUCCESS.

Functions with deviant or limited behavior

These include:

- UTLGetConfiguration - Returns the name of the currently running and API connected Host On-Demand Configuration.
- UTLGetConnectionStatus - Only types UTL_XSTATUS, UTL_CONNECTION, and UTL_ERROR are supported
- UTLGetSessions,UTLListSession - Recognize only a difference between configured and running sessions. UTL_GETCONFIGURED and UTL_GETCONFIGUREDCOUNT will return all sessions identified by the Settings Utility, and all other settings will return sessions that are running and are connected to the host.
- UTLGetEmulatorVersion - Returns the minimum supported version of Host On-Demand

- UTLRunEmulatorMacro - Runs a previously defined Host On-Demand macro

IBM Host On-Demand Utility Bridge

This was the first iteration at a conversion tool for migrating applications written to the Attachmate EAL API and was implemented to support Visual basic applications only. For serviceability reasons, this was absorbed into the EHLLAPI bridge and was subsequently enhanced to allow migration for applications written in any language and to add functional support. Many of the limitations of the Utility Bridge have been addressed in this new implementation. If you are using the Utility Bridge, then there are some steps that must be performed to migrate over to the EHLLAPI Bridge.

Modifications to apps that have already been migrated over to the Utility Bridge are minor. No function name alterations are necessary, but the parameters provided to some functions have changed and are as follows:

Functions:

- utl_StartSession() - In the Utility Bridge this function must take a URL. For this implementation the URL must be replaced with a Session Letter, as is consistent with the original API, and that has been defined with the settings utility.

Additional Steps:

- The settings utility must be used to define Session Letter Associations, and the Startup Program and Host On-Demand URL must be designated.
- The original Utility Bridge must be un-installed. The install for The EHLLAPI Bridge will do this automatically.

The following functions were unsupported in the Utility Bridge, but *are* supported with this implementation:

- StartSession - Behavior was inconsistent with original API
- GetSessions - Now supported
- RegisterClient - Now supported. This function is required before all other function calls are made.
- UnregisterClient - Now supported
- WaitForHostConnect - Now supported
- AddWaitForHostConnect - Now supported
- WaitForHostDisconnect - Now supported
- AddWaitForHostDisconnect - Now supported
- ListSessions - Now supported

- GetSessionHandle - Now supported
- GetSessionStatus - Now supported
- SessionOff - Now supported
- SessionOn - Now supported

Macro Conversion Users

The Utility Bridge also included tools for converting and running Attachmate Macros on Host On-Demand. These tools are now delivered and supported separately. If you are currently using the Macro Conversion Utility, be advised that this installation will uninstall the Utility Bridge causing the converted macros to no longer run. The two versions of the bridge have conflicting files, and cannot coexist as installed.

If you must retain that functionality you can do one of the following:

- Rename the install directory for the Utility Bridge SDK. This will prevent the uninstall from removing the files.
- Reinstall the Utility Bridge SDK after installing this software. If you choose this option, be careful to not reinstall the Utility Bridge DLLs, or make sure that the path statement has the EHLLAPI Bridge install directory first.

The Binary Updater

Programs for which source code is unavailable can still be run against the EHLLAPI Bridge extensions to support Attachmate EAL programs. If the application was written with C/C++, it is likely that it was linked implicitly and would likely be runable as is. However, if the program was written with any other language or was linked explicitly in the code, then the program will be looking for specific symbols in ATMAPI32.DLL to operate. Those symbols are stored as strings in the compiled executable binary, but the values are only important to the logic of the program. With the BinaryUpdater tool, it is possible to alter the value of the string without compromising the integrity of the binary file.

To Use BinaryUpdater:

- Locate the BinaryUpdater.exe in the install directory of the EHLLAPI Bridge.
- Double-click the **BinaryUpdater** icon to start the program.
- Type the name of or browse to the program that must be modified in the field labeled as `Load File`.
- Click **Load Binary**. This loads the binary file into memory. The List box in the center of the dialog should activate.
- If the program was written and compiled with Visual Basic, check the box labeled **Search All Sections**. For most programs, the strings will be stored in

the .data segment of the program, however, if the program was written with Visual Basic, the strings will be part of a special resource section.

- Type the pattern for which to search in the field labeled `Search for Strings Containing:`. For programs written against EAL the pattern will be `ATM`.
- Click the **Search** button. The list box should fill with all the symbols embedded within the binary that contain the pattern indicated.
- Check the boxes next the symbols that should be altered. Be careful to avoid selecting strings that coincidentally contain the search pattern. Or click the button on the right of the dialog that is labeled **Check All,** and then unselect the inappropriate strings.
- In the field labeled `Replacement Pattern`, type the string that will replace the indicated search pattern. The replacement pattern must be the same length as the search pattern. For converting to use the EHLLAPI Bridge extensions, the pattern should be `UTL`.
- Click **Modify Checked**. All of the strings that have been selected should show the new pattern.
- If the replacements look correct, click **Commit**. This will save the new binary and save a backup of the original. The converted program should now be ready to run with Host On-Demand.

The settings utility

The settings utility is meant to accomplish two things:

1. Identify how to start Host On-Demand if it is not running when a call to Start a Session is made.
2. Make associations between session letters and Host On-Demand configurations. All EHLLAPI and EHLLAPI based APIs require session letters to identify their target sessions. Attachmate’s EAL requires that session letters be preassigned to configurations; this tool facilitates making those assignments.

To Use SettingsUtility:

- Locate the `SettingsUtility.exe` in the install directory of the EHLLAPI Bridge.
- Double-click the **SettingsUtility** icon to start the program.
- Type the name of or browse to the program that will be used to run Host On-Demand. This will usually be Internet Explorer in the Program Files Directory, but can be any program that launches a Host On-Demand Applet instance.

- Supply the URL to the HTML file that contains a Host On-Demand Applet and where the parameter `ENABLE_PCSAPI=YES` has been set through the Host On-Demand Deployment Wizard.
- Type the names of saved session configurations in the fields that are labeled with Session Letters. Valid configurations are those that appear in the Host On-Demand desktop once Host On-Demand is running. Unrecognized names are ignored.
- Click **Apply**.

The settings utility makes changes to the Windows registry. If necessary a system administrator can use the settings utility and then export the keys so that they may be distributed to an enterprise. Success with this assumes that all users have predefined configurations using the same names.

24.8 Programming notes

The following topics relate to programming aids and license limitations.

24.8.1 JARs and CABs

The Java libraries supplied in the Host Access Toolkit consist of the underlying class files packaged into JAR and analogous CAB files. JAR libraries are for Netscape and Java applets, and applications and browsers employing the Java 2 Plug-in. CAB libraries are specific to Internet Explorer.

Deployed custom applications may follow one of two forms. The JAR/CAB libraries are installed on the machine where the Java application is run locally, or some or all of the required libraries may be downloaded over the network at runtime. In either case, these libraries should be digitally signed to denote their level of trustworthiness. The Host Access toolkit supplies both signed and unsigned libraries, distinguished as “debug” and “release” versions.

The “debug” JARs contain extra logging information when problem determination is of primary importance. These JARs are not digitally signed and ideally should not be used in a production environment. Because of the extra debugging code, their size is considerably greater than their “release” counterparts. That makes them less desirable in a network downloadable scenario. The “release” JARs are digitally signed, and do not contain the extemporaneous logging and debugging code.

Any custom libraries used to create an applet should be digitally signed or else the security manager of the browser will deny certain instructions from executing. A valid certificate of the appropriate class must be obtained from a Certificate Authority (CA) such as Thawte Consulting or VeriSign, Inc. Signing the Host Access Toolkit JAR/CAB libraries with your own certificate is prohibited under the Host Access Toolkit license agreement.

Because of the size and organization of the HACLJ and HABJ libraries, the toolkit provides “componentized” JARs and CABs. To minimize the amount of code required to be downloaded/transferred, the Host Access Toolkit partitions the functionality of the APIs into multiple JARs and CABs. It is the responsibility of the developer to decide which JARs/CABs must be incorporated into the application's classpath to provide the required functionality. Refer to the installed documentation for a table of debug and release JARs and which functions are provided in each file:

HACL - toolkit directory\en\doc\hacl\API_users_guide.html

BEANS - toolkit directory\en\doc\beans\API_users_guide.html

The custom applet or application that you write should be packaged into its own library file and digitally signed. Your code will use HACLJ and HABJ classes that reside in their own library files that have a trusted digital signature. Your digital signature certifies the trustworthiness of your custom classes, and the IBM digital signature certifies IBM’s classes.

You should not subclass the HACLJ and HABJ classes, but should implement the needed abstract interfaces. And you should not create new classes within the com.ibm.* package domain without expressed written consent of IBM.

24.8.2 Deploying custom written Java applets

If a customer is going to deploy a custom applet that gets loaded by Host On-Demand, the Java archive must be made accessible to Host On-Demand. There are multiple ways to do this, depending on if you are using download clients, cached clients, or if your are using Java 1 HTML pages or Autodetect/Java 2 HTML pages generated with the Deployment Wizard.

Java 1 clients generated with Deployment Wizard

For cached clients, do the following:

Find the HTML file you have generated using the Deployment Wizard. In this file you will find two sets of tags similar to Example 24-7 and Example 24-8.

Example 24-7 Tag 1

```
document.write('<APPLET ARCHIVE="CachedAppletSupporter.jar, Customer.jar" MAYSCRIPT
NAME="CachedAppletSupporter"
CODE="com.ibm.eNetwork.HOD.cached.appletsupport.CachedAppletSupportApplet" WIDTH="2"
HEIGHT="2">');

document.write('<PARAM NAME="Cabinets" VALUE="CachedAppletSupporter.cab, Customer.cab">');
```

Example 24-8 Tag 2

```
document.write('<APPLET ARCHIVE="CachedAppletSupporter.jar, Customer.jar" MAYSCRIPT
NAME="CachedAppletSupporter"
CODE="com.ibm.eNetwork.HOD.cached.appletsupport.CachedAppletSupportApplet" WIDTH="2"
HEIGHT="2">');

document.write('<PARAM NAME="Cabinets" VALUE="CachedAppletSupporter.cab, Customer.cab">');
```

Add the name of your Java archive in the positions illustrated by the file names Customer.cab or Customer.jar.

For download clients, do the following:

Add the name of your jar/cab files on the line `var hod_Jars=` and `var hod_Cabs=` in the HTML file you have created.

Java 2/Autodetect clients generated with Deployment Wizard

For cached clients, do the following:

You must edit a Host On-Demand javascript file to add your archive to the list of loadable archives. Edit file `HodCachedParms.js` which contains the javascript function shown in Example 24-9.

Example 24-9 Edit the first javascript function

```
function writeAppletCachedClient(appName, codeBase, appWid, appHgt, locale, comps, myURL,
mySearch, cParms, hParms) {

   var hcached_App = '';
   var hcached_Jars = '';
   var hcached_Cabs = '';
   if (appName == 'com.ibm.eNetwork.HOD.JSHostOnDemand') {
      hcached_App  = 'com.ibm.eNetwork.HOD.cached.appletloader.JSCachedAppletLoader.class';
      hcached_Jars = 'JSCachedAppletSupporter.jar,CachedAppletSupporter.jar,Customer.jar';<<<
      hcached_Cabs = 'JSCachedAppletSupporter.cab,CachedAppletSupporter.cab,Customer.cab';<<<
   } else {
      hcached_App  = 'com.ibm.eNetwork.HOD.cached.appletloader.CachedAppletLoader.class';
      hcached_Jars = 'CachedAppletSupporter.jar,Customer.jar';<<<
      hcached_Cabs = 'CachedAppletSupporter.cab,Customer.cab';<<<
   }
```

The **<<<** indicates the modification you will have to make. Replace the `Customer.jar` or `Customer.cab` reference with the name of your java archive.

Next, edit the following javascript function in this same `HodCachedParms.js` file. You will need to add your Java archive to the myArchiveList.

Example 24-10 Edit the second javascript function

```
function writeHTML2(componentList, archiveList, versionList) {

  var myArchiveList = archiveList',Customer.jar'; <<<
  var myVersionList = versionList',+1.0.0.0'; <<<
```

Substitute the name of your jar file for `Customer.jar` and add the +1.0.0.0.

For download clients, do the following:

Edit the HTML file the Deployment Wizard generated. Find the following tag:

```
var hod_jars =
```

Add the name of your JAR file to this line. If you may be using Java2 then be sure to create both a `customer.jar` and `customer2.jar` files.

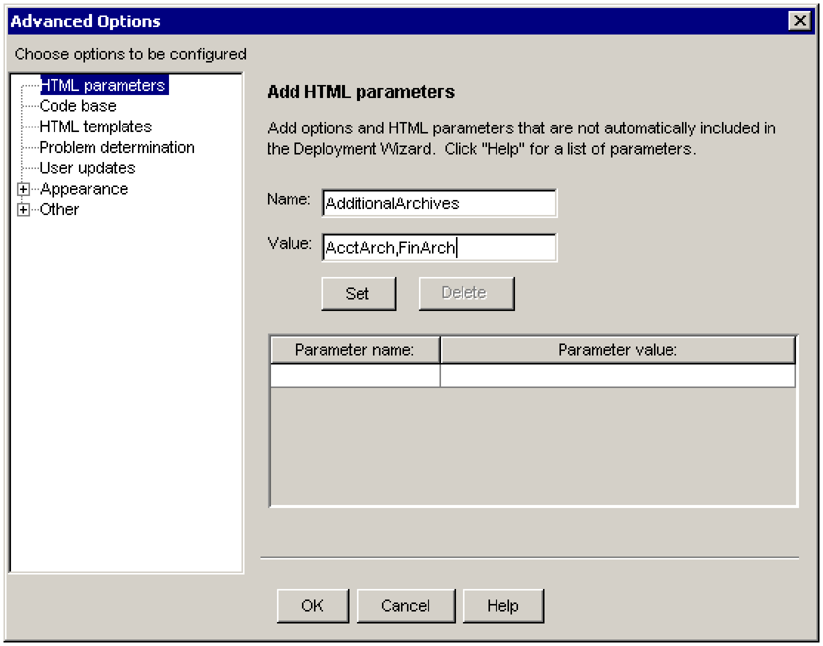
Our javascript code will include a `2` in the name of your JAR file for when Java 2 is detected. The contents of the JAR files can be the same, they just have different names.

AdditionalArchives HTML parameter

The AdditionalArchives HTML parameter is a new parameter added to the Deployment Wizard in Host On-Demand V8. The AdditionalArchives parameter is used to specify the names of your custom Java archives to be downloaded.

You can use the AdditionalArchives parameter when you deploy custom Java 1 (.CAB or .JAR) or Java 2 (.JAR only) archives to a Host On-Demand server. This method of downloading a customer applet works for a cached client, download client, and a Web Start client.

Place your Java archive files in the Host On-Demand publish directory. Then edit the HTML file with the Deployment Wizard. On the Advanced Options panel, click the **HTML Parameters** selection and make the entries as shown in Figure 24-3.



Add HTML parameters

Add options and HTML parameters that are not automatically included in the Deployment Wizard. Click "Help" for a list of parameters.

Name: AdditionalArchives

Value: AcctArch,FinArch

Parameter name:	Parameter value:

Figure 24-3 Specify AdditionalArchives HTML parameter

The Name field must be `AdditionalArchives`, while the Value field specifies your Java archives, separated by commas, without file extensions.

Keep in mind that when using the AdditionalArchives HTML parameter to download custom Java archives, these archives will be downloaded every time the client connects to that HTML file (even when running a cached client). This ensures that Host On-Demand always has the latest versions of your archives. Consider using this method for small Java archives.

24.8.3 Swing components and Host Access Beans

The Host Access Toolkit in HACP 3.0 has introduced a new parallel library set. Developers may use either the “traditional” jdk1.1 set or the “new” java2 set of libraries.

The new java2 version of the Host Access Beans for Java are suited for use in Swing-based applications. There are accessibility features available in this library that are not possible in the jdk1.1 version.

The jdk1.1 Host Access Beans for Java are based upon the Abstract Windowing Toolkit (AWT) components. IBM recommends using AWT components with the jdk 1.1 Host Access Beans. Sun Microsystems warns that incompatibilities may exist when combining components from both the AWT and Swing libraries.

For more information about the caveats of mixing Swing and AWT components, go to the following site:

`http://java.sun.com/products/jfc/tsc/articles/mixing/index.html`

Our experience has shown that there are cases where embedding a jdk1.1 Terminal bean in a java.awt.JFrame experiences difficulties. If you must use this mixture, we recommend experimenting with the order of statements used to build the custom terminal-containing display frame. We have noted that the “permissive” order may vary according to both platform and SDK version service release.

24.8.4 Subclassing and additional notes on licensing issues

Certain uses and practices are not supported or are prohibited by the IBM License Agreement.

Subclassing classes and beans

Subclassing is an object-oriented approach for extending or overriding the functionality defined by a particular class. The Java programming language allows the classes and beans provided in the Host Access Toolkit to be subclassed and public methods to be overridden (if not marked “final”). There are certain classes, such as abstract interfaces, that must be implemented with developer code. But in the main, subclassing and overriding of published HACLJ classes and HABJ beans is not recommended and is not supported by IBM. Design your JavaBeans and classes to use IBM classes and beans without subclassing and overriding them.

Use of unofficial APIs

While allowable by the Java programming language, IBM will not support any use of any class not identified by the official API documentation. Many classes in IBM libraries are “public” in the Java sense, but have been intentionally excluded from the published Javadocs. Therefore, any class that does not appear in the toolkit Javadocs should not be called or programmed directly.

Re-packaging of Host Access Toolkit JARs

While allowable by the Java programming language and available tools, the Host Access Toolkit JARs and CABs for both HACL for Java and the Host Access Beans for Java may not be re-packaged. IBM supplies a set of digitally signed JARs and CABs that internally assert certain needed permissions under a security manager. The Java code composing your classes, beans, packages, applets or applications may need to be digitally signed and to explicitly assert the proper permissions to work correctly under a security manager.

24.9 Custom Applications with Cache Support

The Host On-Demand (HOD) server provides optional support for caching HOD-specific libraries on the client workstation. This mechanism operates for custom applications implementing one of these interfaces:

com.ibm.eNetwork.HOD.common.cached.LoadableAppletInterface (refer to 24.9.1, “The essentials of a LoadableAppletInterface application” on page 900)

com.ibm.eNetwork.HOD.common.cached.WSLoadableAppletInterface (refer to 24.9.2, “The essentials of a WSLoadableAppletInterface application” on page 903)

com.ibm.eNetwork.HOD.common.cached.LoadableJSAppletInterface (refer to 24.9.3, “The essentials of a LoadableJSAppletInterface application” on page 905)

The interface that you choose will depend on the requirements of your custom applet/application. For a cached applet, use LoadableAppletInterface. For a Web Start application, use WSLoadableAppletInterface. And if you need to interact with the host sessions through Java Script, use LoadableJSAppletInterface.

Your application must extend a descendent of java.awt.Component, such as Panel or JPanel, to be visible.

You can develop custom applications of these types using the Host Access Class Library (HACL) and Host Access Beans for Java (HABJ). When served from the HOD server, the libraries for HACL and HABJ will be cached on the client workstation. This facility will not cache or version manage your non-HOD custom libraries. Each time the custom application is started, your custom libraries will be downloaded.

Your custom application libraries should reside in the HOD published directory. Do not combine them into any of the HOD libraries, because that is not permitted by your license agreement. Reconstituted Host On-Demand libraries will be rejected by the caching mechanism.

The caching mechanism does not require that your libraries be digitally signed with a Certificate Authority-derived certificate. That requirement will depend on whether your application code needs Security Manager intervention to invoke privileged execution.

The browsers supported are those that Host On-Demand supports.

Java1 versus Java2

LoadableAppletInterface and LoadableJSAppletInterface are supported in the “java1” and “java2” HOD modes. In the “java1” mode, you may use either loose classes or archived libraries. The “java2” mode requires a JAR archive.

WSLoadableAppletInterface, based on Java Web Start, is a Java 2-only technology. Your custom libraries must be in a JAR archive.

The “"java1” mode uses the native jdk1.1 Java Virtual Machine of the browser. The “java2” mode requires installation and configuration of a Java2 Plug-in.

24.9.1 The essentials of a LoadableAppletInterface application

> **Note:** The LoadableAppletInterface API was introduced into the Toolkit in HACP V3.0 in conjunction with HOD 7.0. The procedure for setting up a custom LoadableAppletInterface application has been simplified. An application written and compiled with HOD 7.0 libraries should recompile and run under HOD 8.0 without modification.

An modified HTML page created with Deployment Wizard can launch an application implementing the LoadableAppletInterface interface. First, the browser loads and launches a HOD-proprietary cached applet loader class. Then that class loads and launches your custom LoadableAppletInterface class.

The Deployment Wizard-based “front” HTML contains the following line:

```
var hod_AppName='';
```

You customize it by filling in the name of your custom application that implements the LoadableAppletInterface interface:

```
var hod_AppName='my_custom_app_name';
```

During the Deployment Wizard process, you will specify an HTML parameter, “AdditionalArchives”, that names the archive file(s) containing your custom code.

What the browser does and does not know

The browser Java Virtual Machine (JVM) loads and launches the proprietary cached applet loader class. The browser is unaware that the loader class has loaded and launched your custom class.

For this discussion, the cached applet loader instance is referred to as theRealApplet. It is the “real applet” because the browser loaded and launched it. The browser is only aware of theRealApplet.

Your custom application is a child of theRealApplet. The relationship is supported by four interface methods shown in Example 24-11.

Example 24-11 Interface methods for LoadableAppletInterface

```
public void setApplet(Applet theRealApplet);
public void init();
public void start();
public void stop();
```

Three of these methods, init(), start() and stop() have the same meaning as the analogous methods in java.awt.Applet.

The method setApplet(Applet theRealApplet) Is Called First

When the cached applet loader loads and launches your custom application, the first method called is setApplet(Applet a). The cached applet loader passes in a reference to itself. The following is an example of custom application code:

Example 24-12 setApplet method

```
...
protected Applet theRealApplet = null;
...
public void setApplet(Applet a) {
   this.theRealApplet = a; //remember who my parent, an applet, is
   }
```

The following is a typical example of your application’s start() method, which is called by the cached applet loader:

Example 24-13 CachedAppletLoader

```
public void start() {
          ... //do some preparation and then...
          if(this.theRealApplet != null ) {
             displayThis(<a GUI component that does the real work>);
          }
```

```
    }

// show the work component in the browser page to the user
    public void displayThis(Component component) {
       this.theRealApplet.removeAll(); // just to be safe
       this.theRealApplet.add(component,null); // insert the new GUI component

       //ask my parent for the top level non-Window Component
       Component topComponent = getTopComponent(this.theRealApplet);
       //visualize me reliably in the browser page
       topComponent.setVisible(true);
       topComponent.validate();
       topComponent.repaint();
    }

// climb the heirarchy as needed
    public Component getTopComponent( Component containingThisComponent ) {
       Component topComponent = containingThisComponent;
       Component nextComponent = topComponent.getParent();
       while( (nextComponent != null) && !(nextComponent instanceof Window) ) {
             topComponent = nextComponent;
             nextComponent = topComponent.getParent();
       }
       return topComponent;
    }
```

The RealApplet is the displayer

The repaint code above is needed to display your custom GUI component. Without it, your custom GUI component may not be visible in the browser page! Notice that there is no requirement that your LoadableAppletInterface application be the visible GUI component. For example, your custom application may be a server that marshals successive GUI components for display in the browser page, only to be removed and replaced by others. Remember to trigger the display of each GUI component after its insertion into "the real applet."

Using the Deployment Wizard

The HOD Deployment Wizard is an integral part of this process. The terse instructions that follow assume that you have familiarized yourself with the Deployment Wizard. Please first read the documentation and practice using Deployment Wizard to configure customized client HTML pages.

The following items described are the additional actions needed in the Deployment Wizard process to create a custom HTML file.

- On the Configuration Model panel, choose the **HTML-based model**.
- On the Host Sessions panel, create a new session of any type. This step is needed to go to next panel.

- On Additional Options panel, choose Java Level (Java1, Java2, or AutoDetect) according to the target mode.
- Choose **Cached Client**
- Click **Advanced Options...** to access Add HTML parameters. Set the parameter Name to AdditionalArchives, and the Value to the name of your custom application archive. Use only the “stem” part of the archive name: Deployment Wizard will fill in .jar or .cab as needed. For example, you should state `myCustApp`, where the name of your custom application archive is `myCustApp.jar` or `myCustApp.cab`.

The Deployment Wizard creates a primary “front” HTML file (and one or more support HTML files) using the name you chose.

This example assumes that you have written a custom application named;lai0.myCustApp, where lai0 is the package name.

In resulting HTML file, look for this line:

```
var hod_AppName = ‘ ’;
```

and change it to:

```
var hod_AppName = ‘lai0.myCustApp’;
```

Running the Custom Applet with Caching the First Time

The first time the client browser accesses the HOD server, the caching mechanism will detect that this *is the first time*. Therefore, the caching operator will download all of the HOD-specific libraries enumerated in the Deployment Wizard step. If this is "java1" mode, a popup dialog will instruct you to close and then relaunch the browser. If this is "java2" mode, the custom application will start immediately. Thereafter, any latency in starting the custom application session is due to the need to re-download the non-HOD libraries. The HOD libraries will be downloaded again only if there has been a version upgrade installed on the HOD server.

24.9.2 The essentials of a WSLoadableAppletInterface application

The code for your hypothetical Web Start application would be identical to the above caching application except that the interface name changes: LoadableAppletInterface becomes WSLoadableAppletInterface. Nothing else changes.

Using the Deployment Wizard

The deployment is a little different in two respects: 1) the specifics of the Deployment Wizard configuration and 2) the file in which you specify the name of the custom application.

The next items describe only the additional actions needed in the Deployment Wizard process to create a custom HTML file.

1. On the Configuration Model panel, choose the **HTML-based model**.
2. On the Host Sessions panel, create a new session of any type. This step activates the **Next** button.
3. On the Additional Options panel, choose **Java2** for Java Level.
4. Choose **Web Start Client**. This triggers a Web Start Setting dialog. Setting the code base value is mandatory. It is similar to following:
5. http://<hod_server>/HOD/.
6. Click **OK** to go back to the Additional Options panel.
7. Click **Advanced Options...** to access `Add HTML parameters`. Set the parameter Name to `AdditionalArchives`, and the Value to the name of your custom application archive. Use only the “stem” part of the archive name: Deployment Wizard will fill in “.jar” or “.cab” as needed. For example, you should state `myCustApp`, where the name of your custom application archive is `myCustApp.jar` or `myCustApp.cab`. Click the **Set button** and then **OK** exit back to the Additional Options panel.

The Deployment Wizard creates a primary “front” HTML file and a specialized supporting jnlp file using the name you composed. You now specify your custom application by modifying the jnlp file.

Change this:

```
<property name_=”hod.CachedClientSupportedApplet”
value_”com.ibm.eNetwork.HOD.HostOnDemand”/>
```

to this, where the package name is `wslai0`, and the custom class to be launched is `WSJava2App`:

```
<property name_=”hod.CachedClientSupportedApplet” value=”wslaiOWSJava2App”/>
```

activates the **Next** button.

The client browser addresses the designated HTML and the standard Web Start establishment process is followed. Because your custom library must be downloaded each time the application is started from the desktop through the Web Start launch icon, the HOD publish directory must be available through its HTTP server.

24.9.3 The essentials of a LoadableJSAppletInterface application

The steps for the LoadableJSAppletInterface are:

1. Create a custom application-launching HTML using Deployment Wizard, being sure to enable the Session Manager API, where you can set in Advanced Option.
2. Write a controlling HTML with your JavaScript logic for accessing the custom application in the other HTML.
3. Create a “front” HTML specifying a FRAMESET relationship between the custom HTML and the controlling HTML.

Although this Interface does not extend LoadableAppletInterface formally in practice, these methods serve the same purpose; see Example 24-14.

Example 24-14 Interface methods for LoadableJSAppletInterface

```
public void setApplet(Applet theRealApplet);
public void init();
public void start();
public void stop();
```

Using the Deployment Wizard

Therefore, the custom application programming details described for a LoadableAppletInterface application all apply here.

The next items describe only the additional actions needed in the Deployment Wizard process to create a custom HTML file:

- On the Configuration Model panel, choose the **HTML-based model**.
- On the Host Sessions panel, create a new session of any type. This step is needed to go to next panel.
- On the Additional Options panel:
  - Choose any type of Java Level (Java1, Java2, or AutoDetect), according to the target mode needed.
  - Choose **Cached Client.**
  - Click **Advanced Options...** to access Add HTML parameters. Set the parameter Name to `AdditionalArchives`, and the Value to the name of your custom application archive. Use only the “stem” part of the archive name: Deployment Wizard will fill in .jar or .cab as needed. For example, you should state `myCustApp`, where the name of your custom application archive is `myCustApp.jar` or `myCustApp.cab`.
  - On this same menu tree, click **Other** to expand the subtree. Highlight Session Manager API, and then check the box to enable the **Session**

Manager API. This is the configuration step which specifically arranges JavaScript access. Click **OK** to exit back to the Additional Options panel.

The Deployment Wizard creates a primary “front” HTML file (and one or more support HTML files) using the name you chose.

This example assumes that you have written a custom application named;jslai0.myJSApp, where lai0 is the package name.

In resulting HTML file, look for this line:

```
var hod_AppName = ‘ ’;
```

and change it to:

```
var hod_AppName = ‘jslai0.myJSApp’;
```

The JavaScript-accessible version of Host On-Demand is being removed and you are substituting your JavaScript-accessible custom applet.

Using CallCustomerFunction(...)

The LoadableJSAppletInterface specifies the entire Session Manager API plus one more method:

- public java.lang.String callCustomerFunction(java.lang.String fncName, java.lang.String parms)

  A method which can be used to extend the API to provide additional functionality. A function name can be passed in (e.g., showColorRemap) and then a list of parameters that can be parsed by the receiving function. Customers can use this API to implement their own custom Java Script API calls.

Your custom application will implement whatever classes and methods that are needed for its functionality. In the case of a Terminal bean-based application, many of the Session Manager APIs might be easily mapped to manipulating your Terminal-based functionality.

However, the callCustomerFunction(java.lang.String fncName, java.lang.String parms) method might be the only JavaScript access you need so that the FRAMESET JavaScript widgets can interact with your cached custom application.

Using the FRAMESET Tag

The FRAMESET HTML file might look something like Example 24-15.

Example 24-15 FRAMESET HTML example

```
<HTML>
<HEAD>
</HEAD>
<FRAMESET rows="85%,15%">
    <FRAME src="JSCustomApplication.html" name="upperFrame">
    <FRAME src="JavaScriptLogic.html" name="lowerFrame">
</FRAMESET>
</HTML>
```

And JavaScriptLogic.html should contains a JavaScript function similar to Example 24-16.

Example 24-16 excerpt from JavaScroptLogic.html

```
function getJsCustomApplication() {
    return parent.upperFrame.getHODFrame();
}
```

The Deployment Wizard-generated HTML, JSCustomApplication.html, already contains this JavaScript function in java1 mode Example 24-17.

Example 24-17 getHODFrame() for Java1

```
function getHODFrame() {
    return self;
}
```

Or, this JavaScript function in java2 mode Example 24-18.

Example 24-18 getHODFrame() for Java2

```
function getHODFrame() {
    return HODFrame;
}
```

JavaScript widgets and interaction logic will reside in one FRAME (HTML). They will use that global reference (above) to the other FRAME (HTML) that is running your custom LoadableJSAppletInterface application. LoadableJSAppletInterface-specific JavaScript calls will be received by your custom application and a value will be returned to the JavaScript caller.

24.9.4 Compatibility of the Java 1 and Java 2 versions

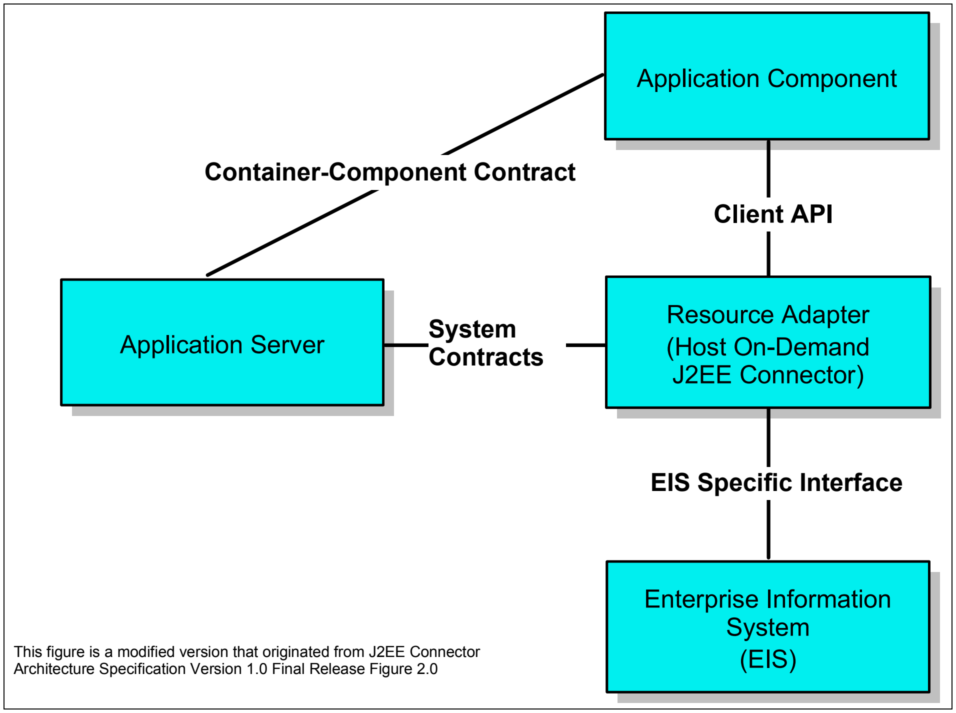
Remember that JDK 1.1-based custom classes run compatibly in a Java 2 environment. Likewise, JDK 1.1-based HOD classes will run compatibly in a Java 2 environment. However, the reverse is not true: Java 2-based HOD classes will fail when run in a JDK 1.1 browser

24.10 Host On-Demand J2EE Connector

The J2EE Connector architecture provides a standard set of services allowing developers to quickly connect and integrate their applications with virtually any back-end Enterprise Information Systems, and to any application servers conforming to the J2EE Connector architecture. This is part of the Java 2 Enterprise Edition.

These services are supplied as Plug-in connectors (sometimes called resource adapters). Before the J2EE Connector architecture was introduced, there was no standard architecture for integrating heterogeneous Enterprise Information Systems (EIS). Host On-Demand users had to use the Host Access Class Library (HACL) to access hosts; other vendors provide specific architectures for this purpose.

Figure 24-4 is a diagrammatic representation of the Host On-Demand J2EE Connector architecture.


Application Component
Container-Component Contract
Client API
Application Server
System Contracts
Resource Adapter (Host On-Demand J2EE Connector)
EIS Specific Interface
Enterprise Information System (EIS)

This figure is a modified version that originated from J2EE Connector Architecture Specification Version 1.0 Final Release Figure 2.0

Figure 24-4 Host On-Demand J2EE Connector architecture

24.10.1 Why use Host On-Demand J2EE Connector?

The Host On-Demand J2EE Connector provides access to 3270, 5250, Customer Information and Control System (CICS), and Virtual Terminal (VT) hosts from the Internet.

The Host On-Demand J2EE Connector is a Java programming interface which conforms to the J2EE Connector Specification Version 1.0 - Proposed Final Draft 2 from Sun Microsystems. This translates to a standard set of services for accessing any system that is J2EE Connector architecture compliant, whether it be the mainframe-based host systems or any other system.

The J2EE Connector is integrated into WebSphere Studio Application Developer-Integration Edition V5.0 and later (WSAD-IE) which provides the tools to capture, generate screens and to develop HOD J2EE Connector applications.

An applet or servlet can be written to use the Host On-Demand J2EE Connector classes for host access over TCP/IP using standard Telnet protocols: TN3270, TN5250, CICS or VT emulation, which otherwise requires the use of a HACL-like API or other emulator APIs.

Since J2EE Connector is a part of the J2EE standards, the following standard system level services between the application server and the back end host system are provided by the J2EE compliant application server.

- Connection Management
- Transaction Management
- Security

Along the lines of JDBC, which is the “de facto” standard to integrate object-oriented Java technology applications with relational databases, the J2EE Connector architecture has become the preferred method to integrate component-based Java technology programs with non-relational back-end enterprise applications.

24.10.2 Host On-Demand J2EE Connector development cycle

Host On-Demand J2EE Connector provides a set of resource adapters that communicate to 3270, 5250, CICS, and VT hosts. These resource adapters (.RAR files) are deployed to a conforming application server, such as IBM WebSphere Application Server, ideally Version 5 and above.

The users can write applets or servlets using the application programming interfaces (APIs) provided in Host On-Demand J2EE Connector through WebSphere Studio Application Developer-Integration Edition V5.0 and later (WSAD-IE). WSAD-IE tools are used to write and test user applets or applications. WSAD-IE is recommended for rapid application development.

These applets and applications are then deployed on to the application server such as WebSphere Application Server. Having done this, we are Internet and intranet ready. Of course, there are security and other parameters that need to be addressed before it really can be used.

24.10.3 Host On-Demand J2EE Connector classes

The HOD J2EE Connector consists of the following classes:

- J2HODConnection
- J2HODConnectionFactory
- J2HODConnectionRequestInfo
- J2HODConnectionSpec
- J2HODInteraction
- J2HODInteractionSpec
- J2HODManagedConnection
- J2HODBaseManagedConnectionFactory
- J2HOD3270ManagedConnectionFactory
- J2HOD5250ManagedConnectionFactory

- J2HODCICSManagedConnectionFactory
- J2HODVTManagedConnectionFactory
- J2HODScreenRecord
- J2HODFieldAttrInfo
- J2HODFieldData
- J2HODFieldInfo
- J2HODFieldRecord
- J2HODScreenableRecord
- J2HODScreenInfo
- J2HODTextAttrInfo

Please refer to the online documentation provided along with Host Access Toolkit for detailed description of these classes. It can be found at:

```
/Program Files/IBM/Host Access Toolkit/en/doc/connector2/
```

24.10.4 Writing a Host On-Demand J2EE connector application

To write an application that is managed and deployed in an application server, use the WebSphere Studio Application Developer - Integration Edition (WSAD-IE) tools. WSAD-IE Version 4.1 or later integrates the Host On-Demand J2EE Connector into its development environment, enabling users to easily write J2EE Connector applications. (Users should use WSAD-IE Version 5.0 or later for the Host On-Demand Version 8.0 J2EE Connector.) Refer to the WSAD-IE documentation for instructions on how to use and write a J2EE Connector application. Once an application is written, it needs to be deployed to an application server. See your application server documentation for detailed instructions on how to deploy application files.

Here are the names, descriptions, and values of some of the properties that are not obvious.

Table 24-4 Non-obvious property information

Property Name	Description	Possible Values
cursorColumn	Which column to place the cursor	0 = leave at current position
cursorRecognizeColumn	Column cursor position to recognize	0 = ignore
interactionVerb	Send, Receive, or Send and Receive	0 = Send 1 = Receive 2 = Send and Receive
keyName	An action key (i.e.: ENTER, PF1)	Use the following rule: #KEY_NAME (i.e.: #ENTER = ENTER, #PF1 = PF1)

Property Name	Description	Possible Values
recognizeColumn	Starting column position of Strings to recognize	integer value within the screen column range
recognizeString	String to recognize	Some texts
screenDescriptors	Screen descriptors	A Vector of ECLScreenDesc class
screenName	Name of screen	Some texts
waitTime	Time limit to recognize a screen	0 = no limit

24.10.5 A sample program

In this section, let us explore a sample program to understand Host On-Demand J2EE Connector and its significance.

The Host Access Toolkit comes with sample programs to understand the HOD J2EE Connector architecture. Well documented and highly self-explanatory programs are provided for TN3270 host access and TN5250 based host access.

The sample programs are found in `\Program Files\IBM\Host Access Toolkit\toolkit\connector2\samples`.

Detailed step-by-step procedures for running these sample programs are available as part of the documentation at `\Program Files\IBM\Host Access Toolkit\en\doc\connector2\J2EEFirstApplet.html`.

Documentation as JavaDoc is available for this API as part of the toolkit. It can be found at `\Program Files\IBM\Host Access Toolkit\en\doc\connector2\index.html`.

24.10.6 Documentation and more information

Detailed documentation is available as part of the Host Access Toolkit package. It is installed on the user workstation when the toolkit is installed. By default it will be installed in `C:\Program Files\IBM\Host Access Toolkit\en\doc`.

24.11 Additional help

A number of Web resources are available for developers using these APIs:

- The IBM Host On-Demand Web page

`http://www.ibm.com/software/webservers/hostondemand/`

- The IBM Personal Communications Web page:

  `http://www.ibm.com/enetwork/pcomm/`

- The Sun Microsystems home page for accessing and downloading various Java APIs and tools:

  `http://java.sun.com/products/`

- The IBM public “Java technology zone”:

  `http://www.ibm.com/developerworks/java/`

- The IBM public “IBM developer kit porting” Web page:

  `http://www.ibm.com/developerworks/java/jdk/index.html`

The following news groups require access to a Usenet newsgroup server, and a client news reader:

- ibm.software.hostondemand
- ibm.software.pcomm

Part 2

Personal Communications Version 5.7

IBM Personal Communications Version 5.7 is the component of Host Access Client Package V3 that provides a full-function terminal emulator. We will limit our discussion of Personal Communications Version 5.7 for Windows to the enhancements made since the base version 5.6

The following chapter describes the major new functions in Personal Communications version 5.7.

25

Enhancements

This chapter describes the enhancements and new functions that have been added to Personal Communications Version 5.7. The following enhancements are discussed:

- Windows Terminal Server improvements (25.1, “Windows Terminal Server improvements” on page 919)
- IPv6 support for Telnet connections (25.2, “IPv6 support for Telnet connections” on page 924)
- Connection timeout improvements (25.3, “Connection timeout improvements” on page 925)
- Multiple screen collection printing (25.4, “Multiple screen collection printing” on page 928)
- Visual enhancements to OIA and Poppad (25.5, “Visual enhancements to OIA and Poppad” on page 933)
- Disabling Standby/Hibernate prompt (25.6, “Disabling standby/hibernate prompt” on page 936)
- Tivoli changes (25.7, “Tivoli changes” on page 936)
- 3270 host application name in the title bar (25.8, “3270 host application name in the title bar” on page 937)
- SNA node configuration changes (25.9, “SNA node configuration changes” on page 938)

- SNA cryptography support (25.10, “SNA cryptography support” on page 942)
- Transport Layer Security protocol support (25.11, “Transport Layer Security protocol support” on page 948)
- Macro enhancements (25.12, “Macro enhancements” on page 950)

For a review of enhancements included in previous releases of Personal Communications, please see *Host Access Client Package Update*, SG24-6182-01.

25.1 Windows Terminal Server improvements

The major objective of this item was to enable certain PCOMM functions to behave predictably when they run under the Windows Terminal Services (WTS) environment. While a majority of the functions related to the display behavior of the emulator and Telnet connectivity by design work under the WTS environment, SNA specific functions were enhanced to create a more robust behavior.

25.1.1 Terminal Services overview

Windows Terminal Services is a feature that allows more than one user to log on to a Windows machine. This feature is available as an add-on to Windows NT, and it is included in Windows 2000 Advanced Server, Windows XP, and Windows .NET.   Users can log on to the Windows machine from the console (the screen physically attached to the Windows machine) or from a “remote desktop client.” Microsoft ships a version of the “remote desktop client” with its WTS enabled products. This version of the client will run on any Windows machine. On Windows XP and Windows .NET, more than one user can log on at the console, although only one of the logged on users will be able to see their desktop at any time. This function is called “fast user switching.”

In a WTS environment, each user who is logged on gets a WTS Session ID. The user logged on at the console physically attached to the machine is always Session 0. Session IDs for users logged on at WTS clients begin with Session 1. By default, programs running in one WTS session will have no knowledge of programs running in other WTS sessions. This allows most applications that were designed to run on non-WTS machines to run on WTS machines without any changes. Each WTS session can run its own instances of the application without ever knowing if or when that same application will runs in another WTS session.

The following figure shows the **Process** tab in the Windows Task Manager display. Note the WTS user names and associated session IDs.

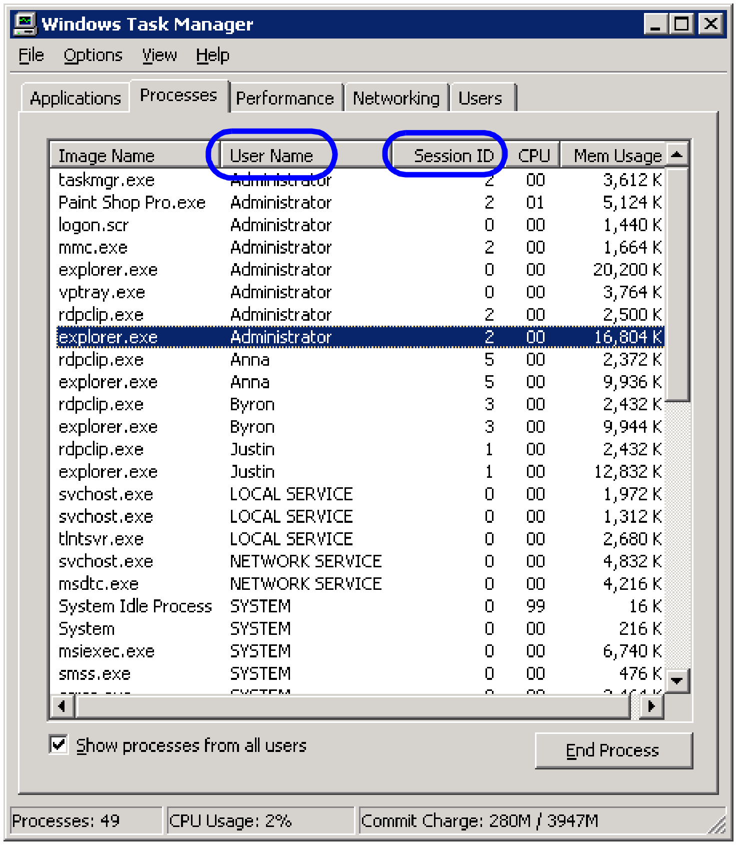


Image Name	User Name	Session ID	CPU	Mem Usage
taskmgr.exe	Administrator	2	00	3,612 K
Paint Shop Pro.exe	Administrator	2	01	5,124 K
logon.scr	Administrator	0	00	1,440 K
mmc.exe	Administrator	2	00	1,664 K
explorer.exe	Administrator	0	00	20,200 K
vptray.exe	Administrator	0	00	3,764 K
rdpclip.exe	Administrator	2	00	2,500 K
explorer.exe	Administrator	2	00	16,804 K
rdpclip.exe	Anna	5	00	2,372 K
explorer.exe	Anna	5	00	9,936 K
rdpclip.exe	Byron	3	00	2,432 K
explorer.exe	Byron	3	00	9,944 K
rdpclip.exe	Justin	1	00	2,432 K
explorer.exe	Justin	1	00	12,832 K
svchost.exe	LOCAL SERVICE	0	00	1,972 K
svchost.exe	LOCAL SERVICE	0	00	1,312 K
tlntsvr.exe	LOCAL SERVICE	0	00	2,680 K
svchost.exe	NETWORK SERVICE	0	00	4,832 K
msdtc.exe	NETWORK SERVICE	0	00	4,216 K
System Idle Process	SYSTEM	0	99	16 K
System	SYSTEM	0	00	216 K
msiexec.exe	SYSTEM	0	00	6,740 K
smss.exe	SYSTEM	0	00	476 K

☑ Show processes from all users

Processes: 49 CPU Usage: 2% Commit Charge: 280M / 3947M

Figure 25-1 Task manager showing user programs and WTS Session IDs

However, there is functionality in PCOMM that needs to run as a machine-wide process, not as a single user process. The functions are:

- SNA node startup and shutdown
- SNA node's support of transaction programs
- Trace facility

25.1.2 SNA node and transaction programs

A transaction program (TP) is a set of instructions that uses Advanced Program to Program Communication (APPC) or Common Programming Interface for Communications (CPI-C) communication functions. By using these functions, your applications can communicate with other applications on the network. For more information on TP concepts, refer to the publication *Client/Server Communications Programming*. In a traditional single user PC environment, an

SNA node can process the Attach for a TP and spawn it in the logged on user's context or in the SYSTEM context. However, in a WTS environment, it becomes important to determine under which user's context the TP programs should run as there are multiple users logged on.

Understanding Program Contexts

In Windows, every process has a security context (also called *account*) associated with it. This context determines the access to the resources that a process can have. The context is derived from the user credentials/rights that the administrator sets. For example, if a user starts a program (hence, creating a process), the user's context becomes the program's context. There is also a predefined context called the SYSTEM (also called LocalSystem) which has extensive privileges on the local computer. Typically, services and programs started by services run under this context (as they are not started by any user).

One of the problems with the previous versions of PCOMM was that if the administrator needed to switch the TP context from user to SYSTEM, they would have to reboot the machine to restart the node in the SYSTEM context. In a WTS environment, this is not a feasible restriction as rebooting will log off all the existing users.

SNA node startup and shutdown options

SNA node configuration has been enhanced to have more control over the startup and shutdown of the node. The SNA Node configuration utility has the AutoStart and AutoStop options that can be set to various values through the **Edit -> SNA Node preferences** dialog. Refer to Figure 25-2.

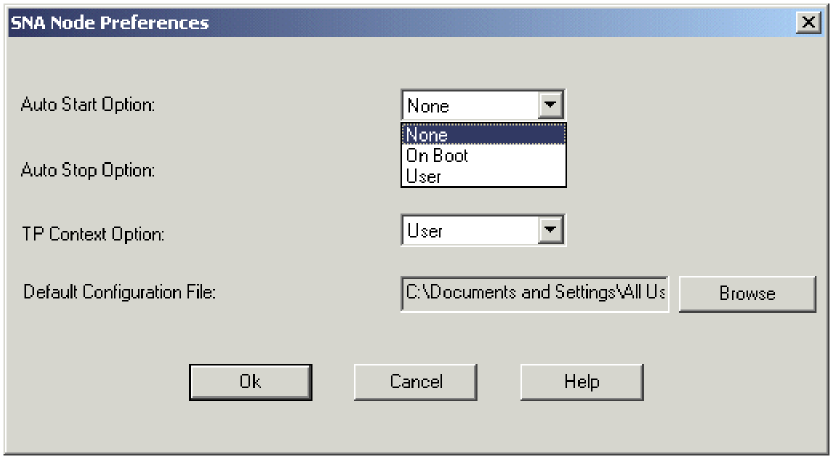
AutoStart option

The AutoStart option controls the startup of the node. It can be set to **None**, **On Boot** and **User**.

If **On Boot** is selected, the node starts when the machine is started. If **User** is selected, whenever the first user logs on to the machine, the SNA node gets started. If **None** is selected, the node must be started manually by the user.

AutoStop option

The AutoStop options define when the node will be stopped. It can be set to **None, TP User, User, Last User.**



SNA Node Preferences

Auto Start Option: None

Auto Stop Option:

TP Context Option: User

Default Configuration File: C:\Documents and Settings\All Us

Figure 25-2 The AutoStart option to control SNA startup.

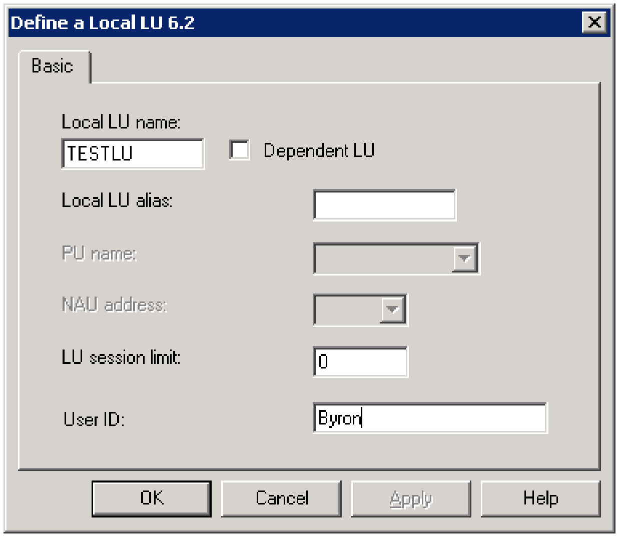
If **None** is selected, the node must be manually stopped. **TP User** is defined as the user who starts the SNA node. So when the user whose logon or who manually started the node logs off, the node is stopped. **User** option implies that if any user logs off, the node will be stopped. This is not a recommended option in a WTS box, as multiple users would be simultaneously logging on and logging off. The **Last User** option stops the node when the last user in the system logs off. If this option is used in conjunction with the AutoStart **User** option, it ensures that the Node is run when only when there are logged on users.

Transaction program context settings

The TP Context Option (see Figure 25-2) defines under which user's context the Transaction Programs started by the SNA node (for Attach) will run in a multiple user environment. There are two values that the option can take, **System** and **User**. If **System** is chosen, the TPs are always run in the SYSTEM context. If the administrator has logged on to Session 0, then the TPs running in the SYSTEM context have access to the Session 0's desktop and all windows created by the TPs are directed to it. If the **User** option is selected, the TPs run in the context of the TP User. The TP User is defined as the user who starts the SNA node. If that user logs off, the TP User becomes the user who has been logged onto the system for the longest time. If the SNA node was started on boot, then the TP User becomes the first user who logs on. Transaction programs have access to the TP User's desktop. If there is no user logged on, and the TP Context Option is set to the **User**, the TP's Attach fails.

There is an option where the administrator can have transaction programs run under specific user contexts. The administrator can define a specific user ID in a Local LU6.2 definition.

All TPs running using the LU will run in the specified user’s context and have access to the user’s desktop. This gives the ability to run the TPs in multiple-user contexts. If the user specified is not logged on, the TP does not run and the attach fails. The value **SYSTEM** also can be specified as a user ID. The TPs running under the LU will run in the SYSTEM context. If a user ID has been specified in Local LU6.2 definition, then the TP Context option set in the SNA node preferences dialog will be ignored for that LU. For LUs where the user ID has not been specified, the TP context settings will be used.



Local LU name: TESTLU

☐ Dependent LU

Local LU alias:

PU name:

NAU address:

LU session limit: 0

User ID: Byron

Figure 25-3 UserID Byron associated with the Local LU name TESTLU

In Figure 25-3, all TPs running in TESTLU will run under the user Byron’s context if the user is logged on.

25.1.3 Trace facility

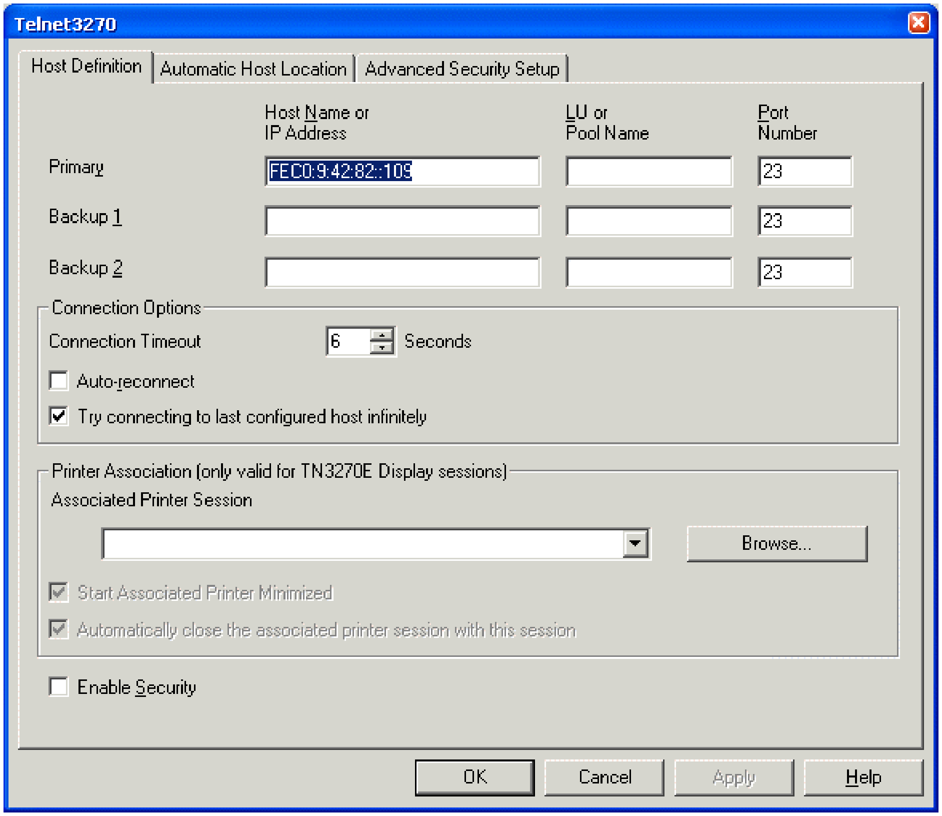
In a Windows Terminal Services (WTS) environment, APPN and APPC tracing can be done only by the user logged on to Session 0. Each user can run their own trace facility, which gives information from that user’s specific WTS logon session. However, there are trace options that enable tracing from device drivers, which are not associated with any specific WTS logon session. Thus, those options only appear on the trace facility that is started in the WTS Session 0.

25.1.4 Other considerations

PCOMM supports three locations for the data directory to reside in: Per User, Common User and Private. In a WTS environment per user option is advisable as emulator state data (like the last position of the emulator window) across sessions is retained on a per user basis.

25.2 IPv6 support for Telnet connections

For Telnet sessions, Personal Communications Version 5.7 supports IPv6 addresses. This support is available on Windows XP (SP1 or later) and Windows 2003. There is no special configuration needed for reaching a host on the IPv6 network. In the hostname field of the Telnet configuration dialog, one can now enter an IPv6 address. All the connection and security options are the same as an IPv4 host.



Telnet3270

	Host Name or IP Address	LU or Pool Name	Port Number
Primary	FEC0:9:42:82::109		23
Backup 1			23
Backup 2			23

Connection Options

Connection Timeout 6 Seconds

□ Auto-reconnect

☑ Try connecting to last configured host infinitely

Printer Association (only valid for TN3270E Display sessions)

Associated Printer Session

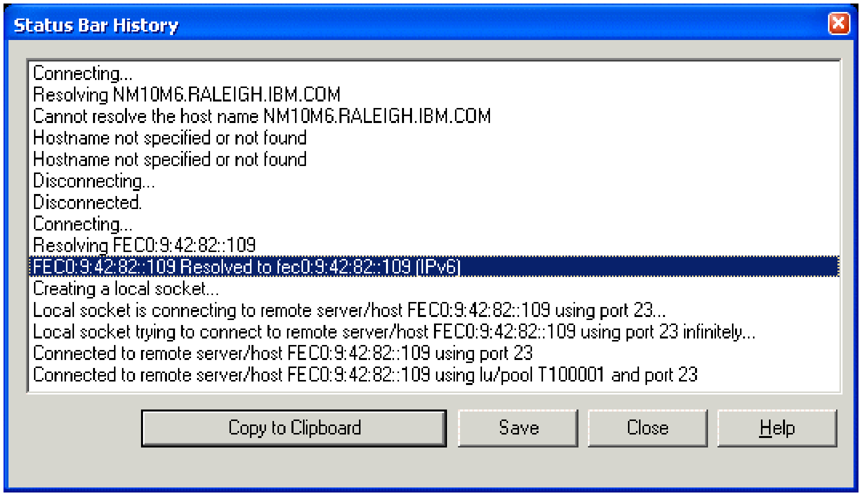
☑ Start Associated Printer Minimized

☑ Automatically close the associated printer session with this session

□ Enable Security

Figure 25-4 Entering an IPv6 address in the communication configure dialog box

If there is a DNS name server that supports IPv6, then one can enter a host name also. Once the emulator tries to connect to the host, it displays in the status bar the address type (IPv6 or IPv4) it uses to connect to the host.



```
Connecting...
Resolving NM10M6.RALEIGH.IBM.COM
Cannot resolve the host name NM10M6.RALEIGH.IBM.COM
Hostname not specified or not found
Hostname not specified or not found
Disconnecting...
Disconnected.
Connecting...
Resolving FEC0:9:42:82::109
FEC0:9:42:82::109 Resolved to fec0:9:42:82::109 (IPv6)
Creating a local socket...
Local socket is connecting to remote server/host FEC0:9:42:82::109 using port 23...
Local socket trying to connect to remote server/host FEC0:9:42:82::109 using port 23 infinitely...
Connected to remote server/host FEC0:9:42:82::109 using port 23
Connected to remote server/host FEC0:9:42:82::109 using lu/pool T100001 and port 23
```

Figure 25-5 Status bar displaying that the address was resolved to an IPv6 address

25.3 Connection timeout improvements

In releases of Personal Communications prior to V5.7, when users tried connecting to a host from a dialup network or a high latency network (like a VPN), they faced the problem of the emulator timing out assuming there was no host. The problem was that the emulator closed the connection too soon even though the host responded to the emulators request to connect. There was no easy way to tell the emulator to use a longer timeout value to take into account the slow connectivity, or wait until the host replied. To accommodate users using slow networks, Personal Communications now provides a timeout mechanism with an option to wait until the host replies. This feature is only available when configuring Telnet connectivity.

25.3.1 Personal Communication’s connection mechanism to a host

One can enter a host address in the configuration dialog as a hostname or an IP address:

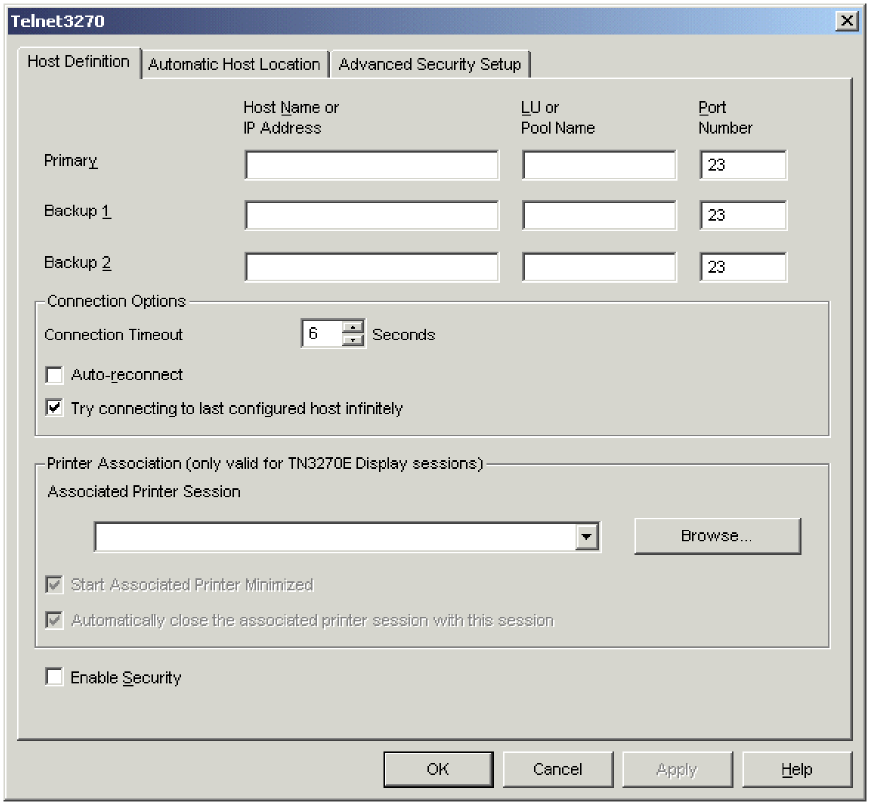
Hostname If a hostname is entered, Personal Communications requests the operating system to check the DNS for its corresponding IP address. If the IP address cannot be resolved, Personal Communications fails the connection to the specified host.

IP address If a valid IP address has been entered, or the DNS was able to successfully resolve the hostname to an IP address; Personal Communications sends a connect request to the host. The connect request waits for the reply from the host for the timeout period. If there is no reply within the timeout period, Personal Communications fails the connection.

25.3.2 Configuring the timeout period

There is a new group called **Connection Options** in the Host definition tab of the Link parameters configuration dialog.

Connection Timeout - The default connection timeout value is 6 seconds (default in earlier versions was 3 seconds). The range is from 1 to 600 seconds. This controls the timeout period on the emulator side for every connect request.



Telnet3270

Host Definition | Automatic Host Location | Advanced Security Setup

	Host Name or IP Address	LU or Pool Name	Port Number
Primary			23
Backup 1			23
Backup 2			23

Connection Options

Connection Timeout 6 Seconds

☐ Auto-reconnect

☑ Try connecting to last configured host infinitely

Printer Association (only valid for TN3270E Display sessions)

Associated Printer Session

Browse...

☑ Start Associated Printer Minimized

☑ Automatically close the associated printer session with this session

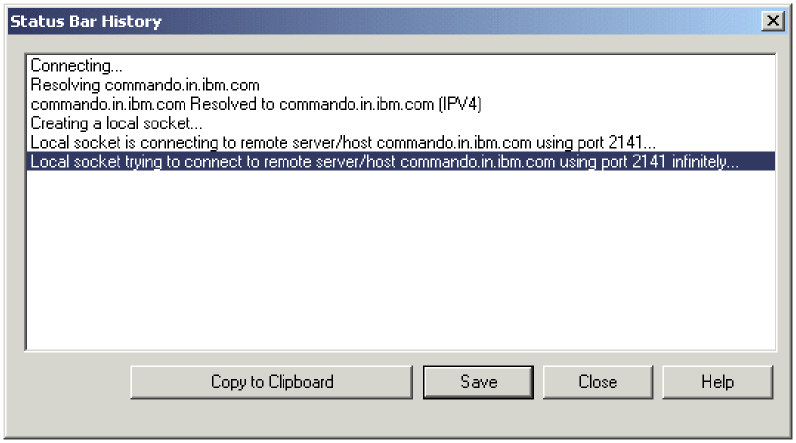
☐ Enable Security

OK Cancel Apply Help

Figure 25-6 The new Connection Options group

Auto-reconnect - Selecting this option forces the emulator to cycle though the Primary, Backup 1 and Backup 2 hosts, and try to connect till it gets connected to any one of them. This option is useful in case the host get disconnected often. This would automatically reconnect to the host.

Try connecting to the last configured host infinitely - This option sends the connection request to the last configured host and waits infinitely till the host responds. The connection timeout value is ignored for this host. If Primary, Backup 1, and Backup 2 are defined, then the last configured host is Backup 2. If just Primary is defined, then it becomes the last configured host. This is enabled by default. When the emulator is trying to connect to the last configured host infinitely, the status bar is updated with the message that it is trying to connect infinitely. Refer to Figure 25-7.



```
Connecting...
Resolving commando.in.ibm.com
commando.in.ibm.com Resolved to commando.in.ibm.com (IPV4)
Creating a local socket...
Local socket is connecting to remote server/host commando.in.ibm.com using port 2141...
Local socket trying to connect to remote server/host commando.in.ibm.com using port 2141 infinitely...
```

Figure 25-7 Status bar history indicating the emulator's attempt to connect infinitely

By their very nature, **Auto-reconnect** and **Try Connecting to the last configured host infinitely** are mutually exclusive. The reason there are check boxes and not radio buttons is that you can turn both the options off. This is possible when the user does not need to auto-reconnect as well as block on the last configured host. This results in the emulator going through the Primary, Backup 1, and Backup 2 hostnames once, and if none of them connects within the configured connection timeout value, the emulator will go to disconnected state (this is the default behavior of previous releases of Personal Communications).

Try Connecting to the last configured host infinitely is an option provided for hosts in a slow network. There is an side effect to this option that the users should be aware of. If the host that the emulator is trying to connect is down, the emulator will still wait infinitely for the host to respond. If the host comes online sometime later after the emulator issued the connect request, the emulator still cannot connect to the host. This is because the host has not received the original connect request to respond to. In this situation, the only option is to manually disconnect from the host. In cases where the host goes down often, it is better to use Auto-reconnect option.

Migration notes

If the profiles are migrated from a previous Personal Communications version, then **Connection Timeout** values are retained at 3 seconds. Also, **Auto-reconnect** values are migrated. On migrating, the **Try connecting to the last configured host infinitely option** is set to off in the migrated profile. So, for migrated profiles, their emulator behaves like the previous versions.

25.4 Multiple screen collection printing

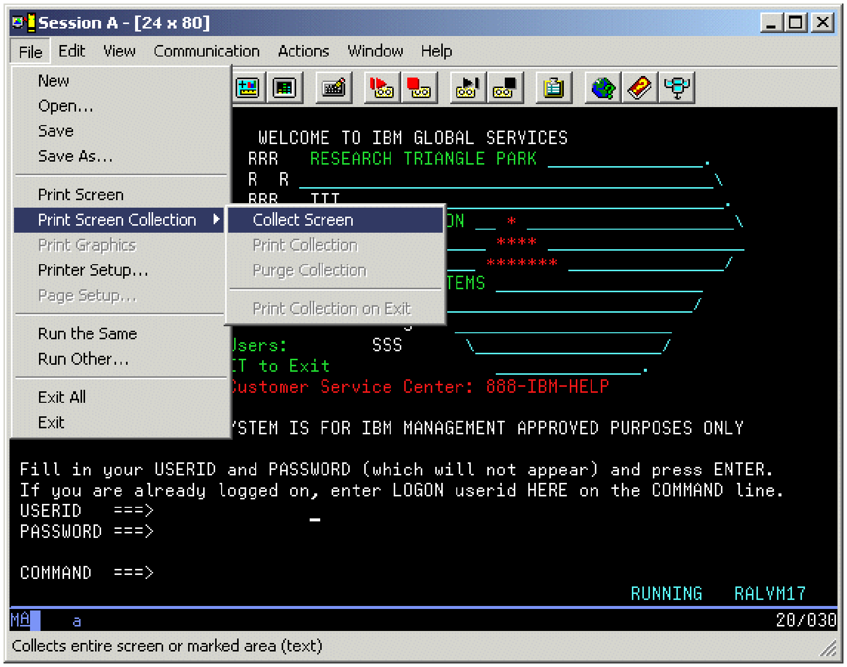
This feature was introduced to help users print multiple screens in a single print job. It also allows users to print multiple screens on a single page. With this feature, the user can collect host screens over a period of time, and then send them to the printer. This can useful in organizations where there is a set of printers in a printer room shared by a number of people. Collecting multiple print screens and printing them as single job as opposed to an individual job per screen saves time and resources.

This functionality can be invoked through menu action, keyboard, poppad, mouse button reconfiguration, and the toolbar. The basic functionality will be explained using menu actions. The following section explains how to remap this function so that it can invoked by other means.

25.4.1 Collecting and printing multiple screens

Collecting screens

The user can start using this function when a session gets connected to the host. To collect a screen use **File -> Print Screen Collection -> Collect** (see Figure 25-8). This adds the current host screen displayed in the session to the collection buffer. The user can navigate to the next screen and use the same procedure mentioned above to collect it.



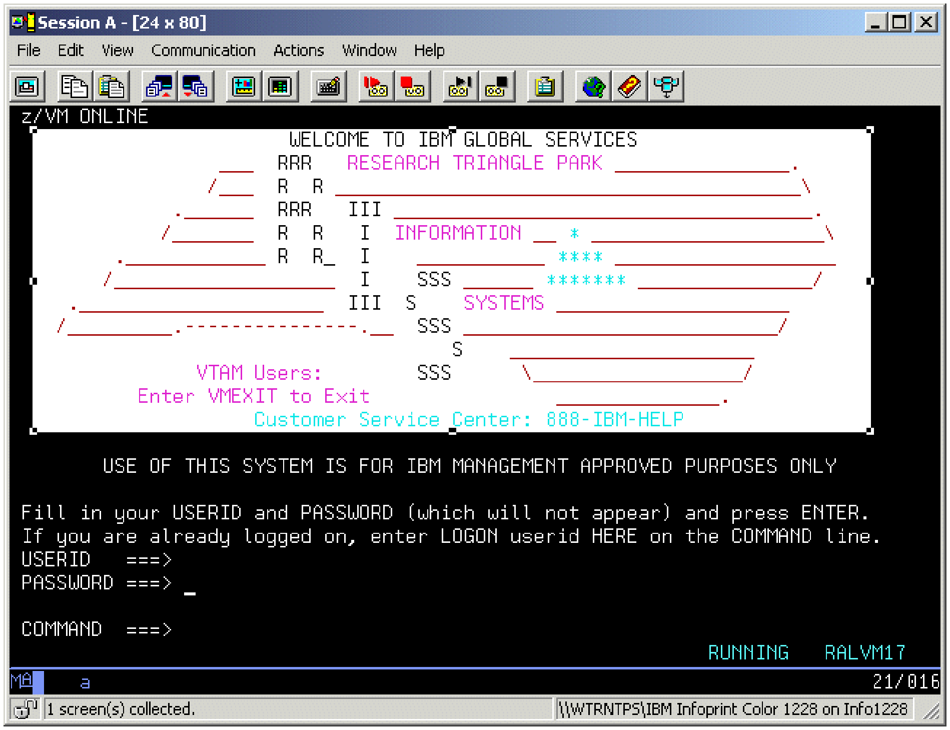
```
  WELCOME TO IBM GLOBAL SERVICES
 RRR   RESEARCH TRIANGLE PARK
 R  R
 RRR   III
                          ON     *
                                ****
                               *******
                          TEMS

Users:          SSS
IT to Exit
Customer Service Center: 888-IBM-HELP

YSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY

Fill in your USERID and PASSWORD (which will not appear) and press ENTER.
If you are already logged on, enter LOGON userid HERE on the COMMAND line.
USERID   ===>
PASSWORD ===>          _

COMMAND  ===>
                                                         RUNNING   RALVM17
MA     a                                                              20/030
```

Collects entire screen or marked area (text)

Figure 25-8 Collecting Host screens

Once there are screens in the collection buffer, the Print Collection, and the Purge Collection menu items grayed out on the pull-downs shown in Figure 25-8 are enabled.

The user can also select partial screens to be copied. To select a partial screen, mark the rectangular area that needs to be collected. Then collect the screen. Note that the number of screens collected is updated in the status bar. Refer to Figure 25-9.



```
 z/VM ONLINE
                       WELCOME TO IBM GLOBAL SERVICES
                 ___   RRR   RESEARCH TRIANGLE PARK _______________.
                /___   R  R  ________________________________________\
               .______ RRR   III ____________________________________.
              /_______ R  R   I  INFORMATION __ * ____________________\
             .________ R  R_  I     __________ **** ___________________
            /_______________  I    SSS ______ ******* _______________/
           .___________________ III  S    SYSTEMS ____________________
          /_______.------------.__  SSS _____________________________/
                                       S       _______________________
                 VTAM Users:        SSS       \____________________/
            Enter VMEXIT to Exit                 _______________.
                       Customer Service Center: 888-IBM-HELP

         USE OF THIS SYSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY

 Fill in your USERID and PASSWORD (which will not appear) and press ENTER.
 If you are already logged on, enter LOGON userid HERE on the COMMAND line.
 USERID   ===>
 PASSWORD ===> _

 COMMAND  ===>
                                                            RUNNING   RALVM17
MA   a                                                                   21/016
```

1 screen(s) collected. \\WTRNTPS\IBM Infoprint Color 1228 on Info1228

Figure 25-9 Collecting a partial screen

Printing the screen collection

Use **File -> Print Screen Collection -> Print** to print the screens. By default, the session will insert a FormFeed between each screen collect, and send it to the printer. After the print job has been submitted to the printer, the screen collection buffer is deleted. The status bar shows the number of screens printed.

Purging the screen collection

If the user needs to discard the screens in the collection without printing them, then the **File -> Print Screen Collection -> Purge** menu option should be used.

Note: The feature works independently of the normal Print Screen function. You can still use Print Screen to print individual screens, while collecting multiple screens and printing them.

25.4.2 Printing multiple screens on one page

An IBM Personal Communications session supports two modes of printing: GDI and PDT. See box below for a brief explanation of both the modes.

Modes of printing in a Session

GDI Mode: In this mode, the print job is submitted to Windows and Windows takes care of the printing. This mode is easy to set up, but does not offer the fine grained control of the printer that certain situations demand.

PDT (printer definition tables) Mode: In this mode, the session talks directly to the printer using the native printer language (represented by the PDT). Binary PDT tables are generated using a text PDF file. The user can modify the PDF file to send commands customized to do special actions. This mode is useful when printing has to be customized for special needs (large batch jobs, printing specific forms, etc.). Refer to *Personal Communications Administrator's Guide and Reference,* SC31-8840-02, and *Personal Communications 3270 Emulator User's Reference*, SC31-8838-02 for details on how to set up the PDT mode.

Printing multiple screens in one page is supported in the PDT mode only. The steps to collect the screens are the same as mentioned above. Instead of sending formfeeds between successive screens, blank lines are sent to the printer. The emulator uses the **BEL** command in the PDF file to specify the number of blank lines that must be sent for separation between screens.

The valid values for the **BEL** command are given in Table 25-1.

Table 25-1 Valid values of the BEL command in the printer definition file

BEL Value in the PDF file	**Explanation**
BEL=00	No separation between pages. Print the next page in the immediate next line.
BEL=FF	One screen per page.
BEL=0xN	N is the number of blank lines to be inserted after printing each page.
BEL=	No value defined for **BEL**. This implies one screen per page.

After changing the PDF with the appropriate BEL value, generate a PDT file and select the generated PDT to be used in the current session. Refer to the PC Admin guide and 3270 Emulator reference for further details on generating the PDT file from a PDF file.

It is important that an appropriate value is used for the **BEL** command. Improper values can result in a screen being split and printed across pages.

25.4.3 Print collection on exit

By default, if there are screens collected and the user disconnects from the host or exits the session, the emulator will print the screen collected till that point. It can be turned off by checking off **File -> Print Screen Collection -> Print Collection on Exit. File -> Print Screen Collection -> Print.** Irrespective of whether the collected screens are printed or not, the buffer is deleted whenever the session disconnects from the host or the user exits the session. If the host is disconnected often, it is a good idea to turn this option off as it prevents the collection from printing prematurely.

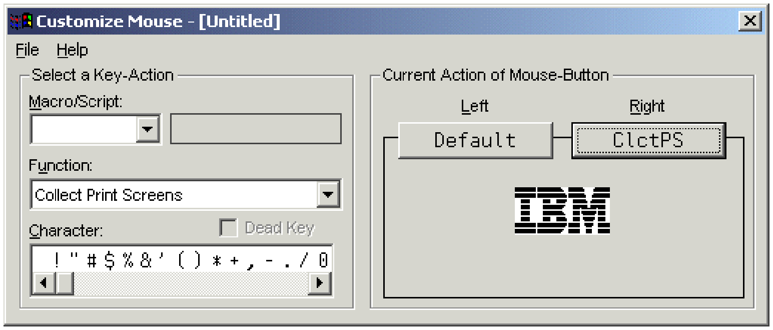
25.4.4 Remapping the toolbar, mouse, poppad, and keyboard

Toolbar

There are four new tool bar items: CollectPS, PrintAllPS, PurgeClCt, PrtOnExit. They can be added to the toolbar and invoked from the toolbar. PS here means the host screen which is also known as the Presentation Space.

Mouse, poppad, and keyboard

Individual elements of the mouse, poppad, and keyboard can be assigned to carry out different emulator functions. There are four new emulator functions, Collect Print Screens, Print Collected Screens, Purge Collected Screens, and Print Collected Screens on Exit. Below is an screenshot of remapping the right mouse button to the Collect Print Screen function.



Function: Collect Print Screens

Left: Default

Right: ClctPS

Figure 25-10 Assigning the right mouse button to Collect Print Screens function

25.4.5 Limitations

- Limited to 3270 and 5250 sessions. VT, BIDI, and DBCS sessions not supported
- Once the collection is printed, the collection is deleted.
- While printing, if the user cancels the print, the print job is cancelled but the collection is deleted.
- The user cannot selectively print the selection.

25.5 Visual enhancements to OIA and Poppad

Personal Communications Version 5.7 has been enhanced to facilitate the use of accessibility devices such as screen readers.

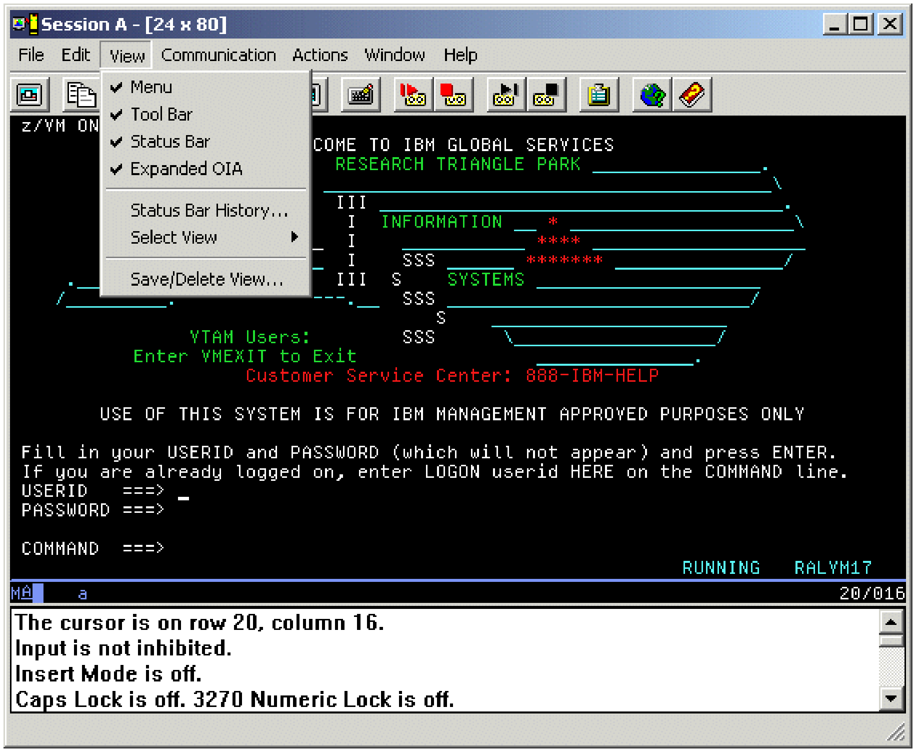
25.5.1 Expanded OIA

The operator information area (OIA) can now be expanded have textual representation of each of the fields. This allows accessibility tools like screen readers to interpret the OIA in a more meaningful fashion. The expanded OIA window drops down below the OIA area of the session window. Each of the OIA fields in the session is represented by one line of text in the Expanded OIA window.

The Expanded OIA by default is de-activated. To activate the Expanded OIA, go to the View Menu and check the **Expanded OIA** item. It can also be activated through system menu. The online help defines the order of explanation of fields in the expanded OIA. Also, if a user hovers the mouse over one of the symbols in OIA area, the text that the symbol represents is displayed in a tool tip.

By default, four lines of OIA explanation text will be visible in the expanded OIA window. You can change the number of visible lines in the expanded OIA from the Windows Setup dialog.

The majority of the screen readers will read the contents of the window that has the active focus. To aid screen readers to read the expanded OIA, one will need to toggle between the Host Presentation space (the session window) and the expanded OIA window. There is a new key map function (**OIA: Toggle to/from focus expanded OIA**) that can be mapped to any key to toggle between the expanded OIA window and the session window.



```
z/VM ON
                    COME TO IBM GLOBAL SERVICES
                      RESEARCH TRIANGLE PARK
                     III
                      I  INFORMATION   *
                      I               ****
                      I    SSS       *******
                     III  S     SYSTEMS
                           SSS
                              S
              VTAM Users:  SSS
         Enter VMEXIT to Exit
                   Customer Service Center: 888-IBM-HELP

        USE OF THIS SYSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY

Fill in your USERID and PASSWORD (which will not appear) and press ENTER.
If you are already logged on, enter LOGON userid HERE on the COMMAND line.
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                       RUNNING   RALVM17
MA     a                                                              20/016
```

The cursor is on row 20, column 16.
Input is not inhibited.
Insert Mode is off.
Caps Lock is off. 3270 Numeric Lock is off.

Figure 25-11 A Session with the expanded OIA

25.5.2 Poppad changes

The poppad (popup keypad) customization interface has been enhanced to provide a simpler way to customize poppads. It is now possible to customize the poppad using the keyboard and drag and drop interface. Its also possible to invoke the poppad using keyboard and change focus to the sticky keypad using the keyboard. Popup keypads have been enhanced to have variable number of buttons in each keypad.

Poppad customization

The first tab in the popup keypad dialog allows one to specify the number of pads that keypad can have (refer to Figure 25-12). The second tab allows you to change the number of rows and columns of buttons in the popup keypad. This release allows one to have variable number of rows and columns for every pad. To change the number of rows or columns for a pad, select which pad you want to change, using the radio buttons at the bottom of the displayed pad, and then change the number of rows or columns to the desired amount. The third tab allows one to assign a function, macro or character to a poppad button. For example, if you need to assign a function, select the desired function and drag it to the button. If you are not using a mouse, select the desired function, then tab to the desired button and press Enter or <space>. The fourth tab allows one to assign colors to the poppad elements.

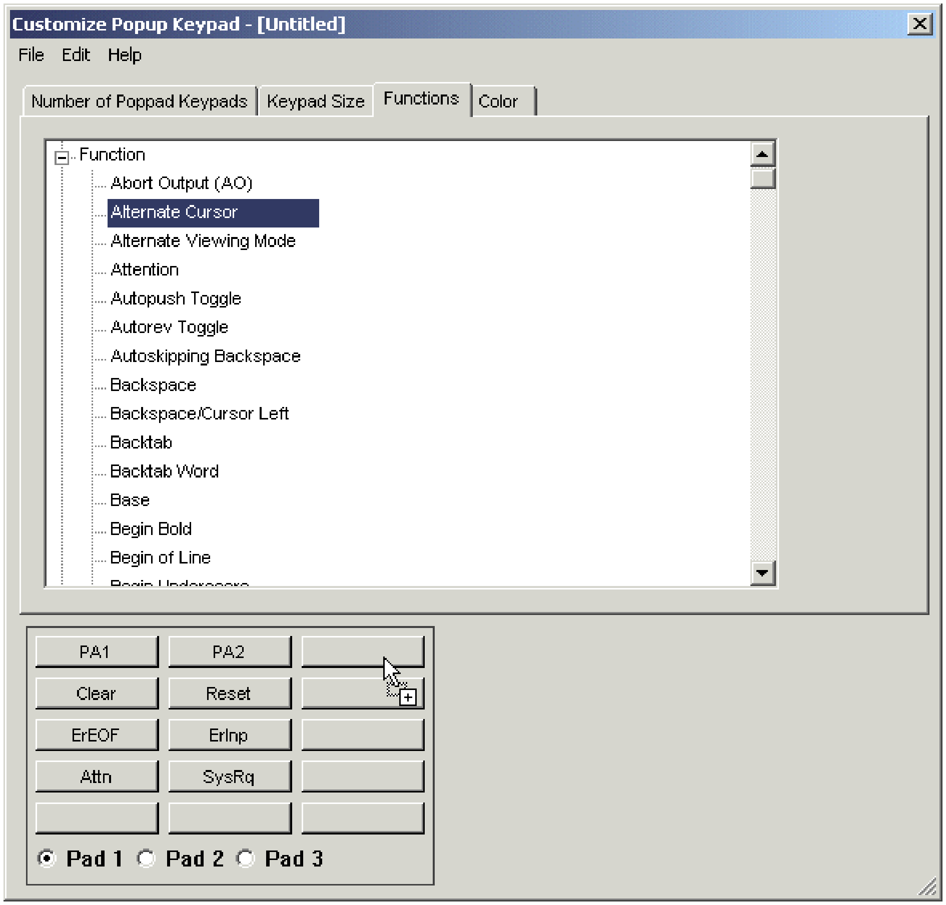


Figure 25-12 New Customize Popup Keypad dialog

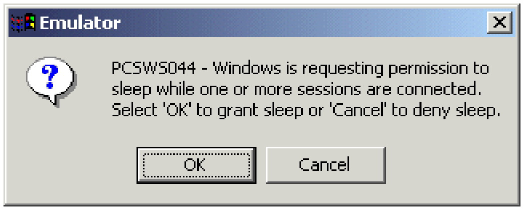
Displaying the popup keypad with the keyboard

Normally, the popup keypad is invoked with a right-click of the mouse. However, there are six new keymap functions to display the poppad, which can be assigned to keys. The **Display Poppad** function displays the last poppad that was shown and puts keyboard focus on it. The functions: **Display Poppad Pad 1**, **Display Poppad Pad 2**, **Display Poppad Pad 3**, and **Display Poppad Pad 4** display a specific poppad and put the keyboard focus on that pad.

A regular poppad exits when you push one of the buttons. But with a sticky poppad, the poppad window remains open until you close it. To get focus to a sticky pad without a mouse, you must map the **Set Focus to Poppad** function to a key. This sets focus to the sticky poppad from the session window. Because you must use the Ctrl-Tab key combination to get focus from the sticky poppad back to the session, mapping the **Set Focus to Poppad** function to the Tab-Ctrl key combination is advised.

25.6 Disabling standby/hibernate prompt

Whenever the system goes to the standby/hibernate state, and the emulator has one or more sessions connected to a host, it will prompt the user permission the go to the standby/hibernate state.



PCSWS044 - Windows is requesting permission to sleep while one or more sessions are connected. Select 'OK' to grant sleep or 'Cancel' to deny sleep.

Figure 25-13 The emulator prompt requesting permission to go to the standby state

In many cases, the users do not want to answer this prompt every time they want they select to sleep/hibernate. To automatically go to standby/hibernate without prompting, the user can select an option **Standby/Hibernate without prompting** in the user preferences manager. The user preferences manager can be invoked from the Windows Start Menu (**Start -> Programs -> IBM Personal Communications -> Utilities -> User Preferences**).

It should be remembered that the connection to the host will be lost when Windows automatically goes to the standby/hibernate mode.

25.7 Tivoli changes

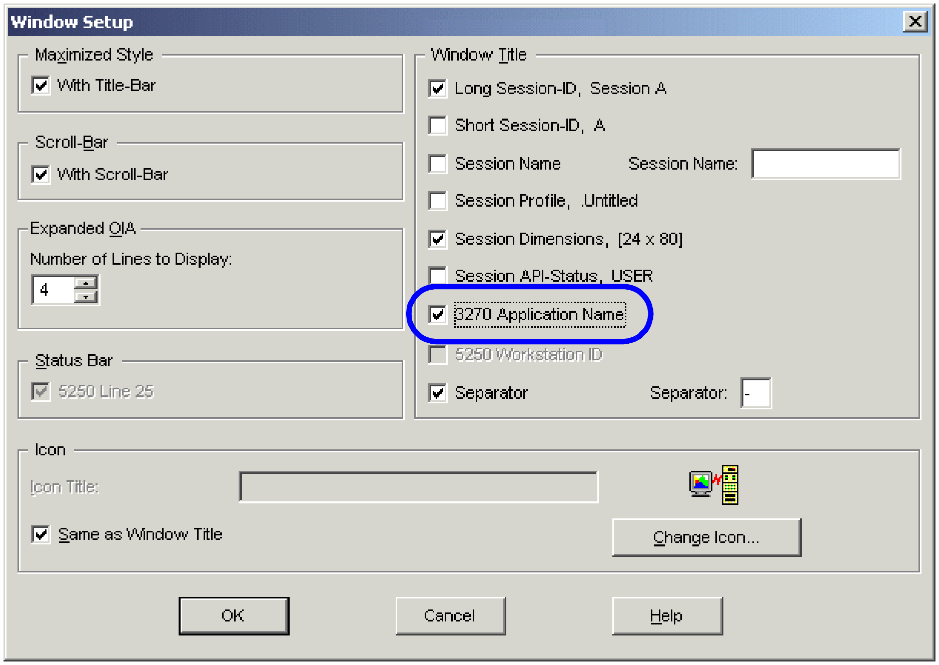
PCOMM has dropped support for the PCOMM Plus module. The plus module used to support remote monitoring, event management, and distribution. Currently, PCOMM only supports Software Distribution using the Tivoli Configuration Manager V4.2.

The new software distribution delivers its support through software packages (.sp). Software packages contains all the data and logic to be installed at an endpoint. The software package editor (supplied by Tivoli) creates a software package, which is then pushed to the end points. The software package for PCOMM can be created using the PCOMM MSI file. The process of creating a software package for PCOMM is documented in *CD-ROM Guide to Installation,* GC31-8079 distributed on the product CD.

25.8 3270 host application name in the title bar

When the emulator connects to a 3270 host application, the host application's name can be displayed in the title bar. This is possible because the emulator receives the application name in the BIND data (or BIND-IMAGE in TN3270E). BIND is part of the SNA protocol; it is not part of the 3270 data stream.

To enable this support, you must select **3270 Application Name** in the Window Setup dialog. See Figure 25-14.



Window Setup

Maximized Style
☑ With Title-Bar

Scroll-Bar
☑ With Scroll-Bar

Expanded OIA
Number of Lines to Display: 4

Status Bar
☑ 5250 Line 25

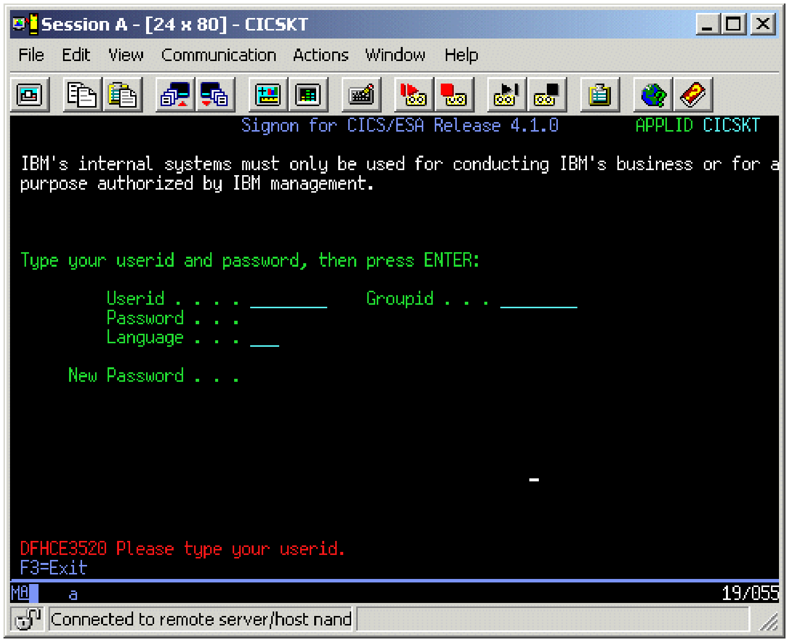
Window Title
☑ Long Session-ID, Session A
☐ Short Session-ID, A
☐ Session Name Session Name:
☐ Session Profile, .Untitled
☑ Session Dimensions, [24 x 80]
☐ Session API-Status, USER
☑ 3270 Application Name
☐ 5250 Workstation ID
☑ Separator Separator: -

Icon
Icon Title:
☑ Same as Window Title

Figure 25-14 Selecting 3270 Application Name

Invoke this dialog from **Edit -> Preferences -> Appearance -> Window Setup**.

This feature is supported for 3270 only. The supported connection types are TN3270E and SNA. This is not supported in TN3270 because no application name is sent in the datastream. No application name is displayed when PCOMM is not bound to a 3270 application (in an SNA connection) or when the communication is disconnected.



```
                                     Signon for CICS/ESA Release 4.1.0         APPLID CICSKT

 IBM's internal systems must only be used for conducting IBM's business or for a
 purpose authorized by IBM management.


 Type your userid and password, then press ENTER:

              Userid . . . . ________      Groupid . . . ________
              Password . . .
              Language . . . ___

        New Password . . .



 DFHCE3520 Please type your userid.
 F3=Exit
MA      a                                                                  19/055
Connected to remote server/host nand
```

Figure 25-15 The application name CICSKT displayed on the tile bar

> **Important:** This feature is available in Personal Communications Version 5.7 CSD1 and above only.

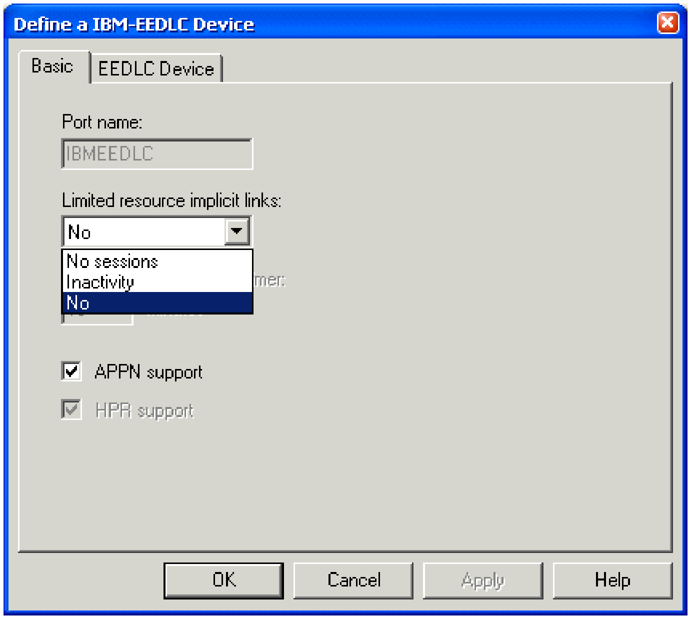
25.9 SNA node configuration changes

Personal Communications Version 5.7 adds non-limited resource support for connection networks using an Enterprise Extender data link control (EEDLC) link.

Connection Networks support establishment of direct sessions between two non-adjacent nodes in an APPN network. A Connection Network can be established using any of the ports (LAN devices) as configured. If an EEDLC device is used in a Connection Network, previous versions of PCOMM always treated the EEDLC device as a limited resource. Both the link and the LU6.2

session’s resources were released when there were no conversations on the LU6.2 sessions (even for a short period of time). This results in the usage of network resources for session termination and re-establishment, which in certain conditions is not acceptable.

In Personal Communications Version 5.7, an EEDLC device has a configuration parameter that controls how the implicit link behaves in case of inactivity. The device can be set up as a limited resource, where the device resources are released in case of inactivity. However, if the device is configured as a non-limited resource, the device will stay alive irrespective of the inactivity. This is controlled by the **Limited Resource implicit links** option under the **Basic** tab of EEDLC device configuration using the SNA Node Configuration utility. See Figure 25-16.



Define a IBM-EEDLC Device

Port name: IBMEEDLC

Limited resource implicit links: No

No sessions
Inactivity
No

☑ APPN support

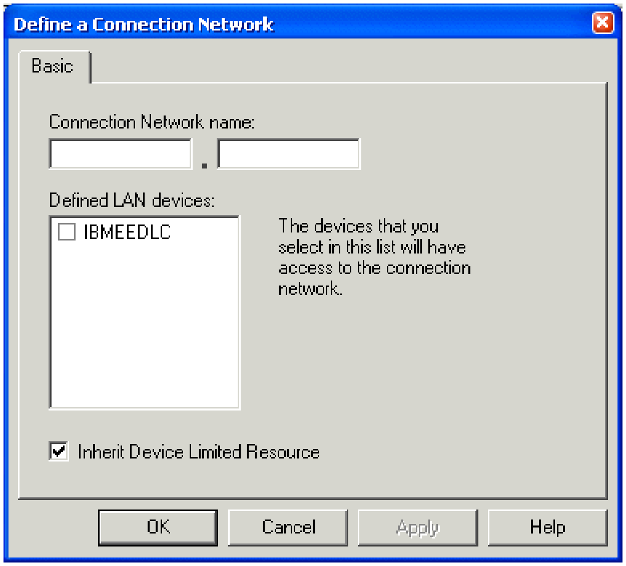
☑ HPR support

Figure 25-16 EEDLC basic configuration with Limited Resource implicit links option

The possible values for this option are:

- **No sessions** - The link disconnects when the last session ends.
- **Inactivity** - The link disconnects when no active sessions are using the link or when no session activity is detected for the period of time specified by the inactivity timer.
- **No** - The link is not a limited resource, and therefore is never automatically disconnected (non-limited resource)

An check box option is provided under the **Basic** tab of Connection Network Configuration - **Inherit Device Limited Resource**. See Figure 25-17. If this is selected, the Connection Network using the EEDLC device will honor the EEDLC device's **Limited Resource implicit links** setting.



Define a Connection Network

Basic

Connection Network name:

Defined LAN devices:

□ IBMEEDLC

The devices that you select in this list will have access to the connection network.

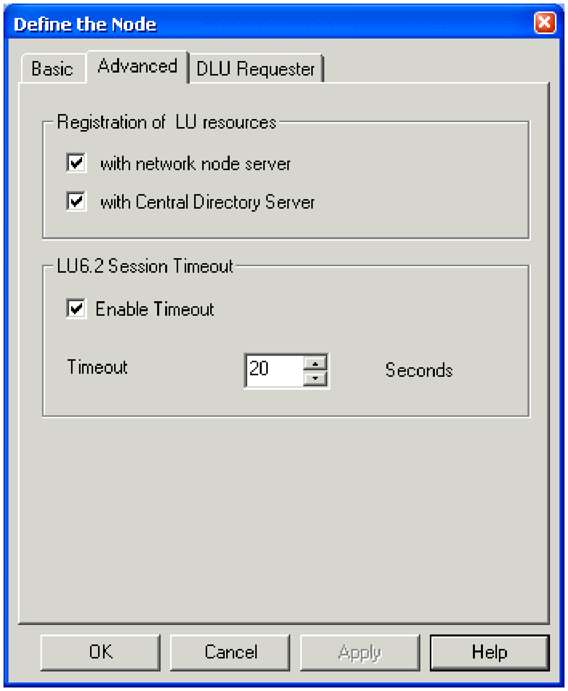
☑ Inherit Device Limited Resource

Figure 25-17 Connection Network configuration w/Inherit Device Limited Resource

To make a Connection Network using an EEDLC device a Non-Limited Resource, set the **Limited Resource implicit links** in EEDLC device configuration to **none** and enable the **Inherit Device Limited Resource** setting in Connection Network configuration. With this setup, the EEDLC link and the LU6.2 session's resources will not be released irrespective of whether sessions are active or not.

25.9.1 LU 6.2 session timeout

Under the node configuration, the users can set the time of inactivity after which the LU6.2 sessions will be timed out. This is provided under the **Advanced** tab of Configure Node in the SNA Node Configuration utility. The default value is 20 seconds. See Figure 25-18.



Registration of LU resources

☑ with network node server

☑ with Central Directory Server

LU6.2 Session Timeout

☑ Enable Timeout

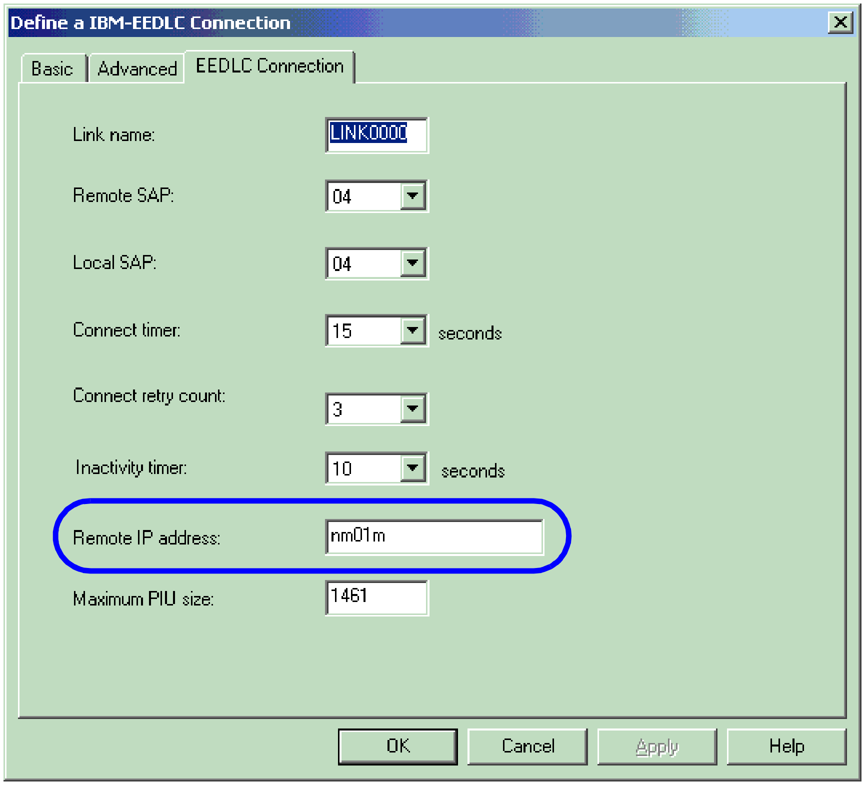
Timeout 20 Seconds

Figure 25-18 Advanced Node Configuration with LU6.2 timeout options

LU6.2 Timeout can be used in conjunction with Non-Limited Resource setting (in Connection Networks using EEDLC), so that the LU6.2 sessions will be brought down when the sessions timeout because of inactivity (otherwise, the sessions remain active forever even if there is no activity).

EEDLC hostname support

The SNA Node Configuration utility will accept hostnames also while configuring a EEDLC connection (Remote IP Address field in the EEDLC Connection tab). In prior versions of PCOMM, only IP addresses were accepted.



Link name: LINK0000

Remote SAP: 04

Local SAP: 04

Connect timer: 15 seconds

Connect retry count: 3

Inactivity timer: 10 seconds

Remote IP address: nm01m

Maximum PIU size: 1461

Figure 25-19 EEDLC configuration: Remote IP address accepts host names

25.10 SNA cryptography support

SNA session level encryption (SLE) enables secure data transfer between nodes running SNA applications. The request units (RUs) for all the SNA traffic across the selected session are encrypted. Software encryption and decryption is implemented by the Application Manager for Data Security (AMDSEC) utility. AMDSEC is a software implementation of the Common Cryptographic Architecture verbs used by SNA session level encryption (SLE). A subset of these verbs, which are required to allow data confidentiality are implemented in Personal Communications.

Because this is a complete software implementation, it will be slower than the conventional hardware-based encryption. Also, since the keys reside on disk, it is less secure than the hardware implementation. SNA SLE is only supported for Windows NT, 2000, and XP platforms. Some of the supported environments are as follows:

- 3270 emulation
- APPC/CPI-C client-server applications
- APPC over TCP/IP
- Sockets over SNA: Encrypted transport sessions

The key-encrypting keys can be added or accessed using the command-line utility **amdsec.exe**, which is available in the Personal Communications installation directory.

25.10.1 Configuring proper key-encrypting keys (KEK)

Enter the key-encrypting keys before performing any operation. KEKs are shared between the LUs for encryption. KEKs reside in key storage (.kek file) and are used to protect data (session) keys when they are sent to the partner node or Logical Unit (LU).

The following commands are available to add or modify these keys:

- **amdsec clear -** This command clears the AMDSEC key storage. All key-encrypting keys are discarded.
- **amdsec pass <new passphrase> -** This command sets the AMDSEC passphrase. Using this passphrase, the key-encrypting keys are secured before they go to the storage file (by encryption). The default passphrase is `amdsec security`.
- **amdsec addkey <label> <key value> <key form> <option> -** adds a key-encrypted key to key storage.
  - **<label>** is the key label for this KEK (up to 5 key label tokens of 8 bytes each) (the rules for naming the labels are explained later).
  - **<key value>** is the KEK value. It must be 16 bytes in hexadecimal (32 hex digits), optionally separated by the - (hyphen) character.
  - **<key form>** is the value *importer* or *exporter*.
  - **<option>** is the value *translate.* Specify this option to have the translate attribute for this key. This parameter is optional. Data key translate is required only when you are running APPN encryption.

  Examples:

  ```
  amdsec addkey cm@lu@im.netid.cpnam1.netid.lunam2
  8182-d4e7-836a-4d6f-8182-d4e7-830a-4d6f importer
  ```

  ```
  amdsec addkey cm@lu@ex.netid.cpnam2.netid.lunam1
  8182-d4e7-836a-4d6f-8182-d4e7-830a-4d6f exporter
  ```
- **amdsec repkey <label> <key value> <key form> <option>** - Some host-side setups support only 8 byte key values. In those cases, duplicate the 8 byte

key to make it a 16 byte key and add that value. This command is used for that purpose. <label>, <key value>, <key form>, <option> have the same meaning as in the **amdsec addkey** command:

Examples:

```
amdsec repkey cm@lu@im.netid.cpnam1.netid.lunam2
8182-d4e7-836a-4d6f-8182-d4e7-830a-4d6f importer
```

```
amdsec repkey cm@lu@ex.netid.cpnam2.netid.lunam1
8182-d4e7-836a-4d6f-8182-d4e7-830a-4d6f exporter
```

- **amdsec list -** lists your KEK labels in key storage.

When entering KEKs, it is often easier to edit the commands in a batch (.bat) file and then execute the command to enter your keys in key storage.

25.10.2 Naming labels for KEKs for dependent LU encryption

The key label when implementing session level encryption for dependent LU sessions uses the following naming convention:

```
CM@LU@IM.mynet1.cpname1.puname.locaddr
```

- **CM** is a constant prefix.
- **@** is a constant delimiter.
- **LU** identifies an LU key-encrypting key.
- **IM** identifies an importer key-encrypting key.
- **netid1.cpname1** is the fully qualified name of the local node where the key-encrypting key will be used.
- **puname** is the PU name of the subarea or DLUR PU, as configured in the Communications Server.
- **locaddr** is the network addressable unit address or local address of the dependent LU. It has to be of the form nnn with possible values from 1 to 255 (for example, 001, 002, 003, . . ., 255).

> **Note:** For encryption of dependent LU sessions, you only need importer KEKs in the Communications Server node, because LUA sessions are always secondary.

25.10.3 Naming labels for KEKs for APPC encryption

The following key labels are used for the key-encrypting keys:

CM@LU@IM.netid1.cpname1.netid.luname

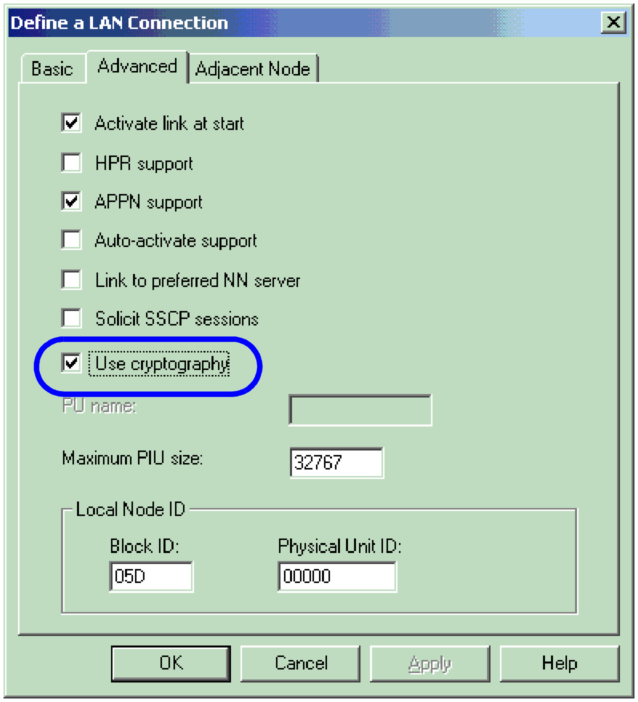
CM@LU@EX.netid1.cpname1.netid.luname

- **CM** is a constant prefix
- **@** is a constant delimiter
- **LU** identifies an LU key-encrypting key
- **IM** identifies an importer key-encrypting key
- **EX** identifies an exporter key-encrypting key
- **netid1.cpname1** is the fully qualified name of the local node where the key-encrypting key will be used.
- **netid.luname** is the fully qualified name of the partner LU

> **Note:** In APPC, an independent LU can initiate a session (primary LU) or it can be secondary when the partner LU initiates the LU 6.2 session. If the LU initiates a session, an exporter KEK is required in key storage. Otherwise, an importer KEK will be used.

25.10.4 Enabling cryptography in SNA node configuration

Open the SNA Node Configuration utility (pcscfg.exe). In the Connection Configuration section of the LU you are planning to use, select the **Use Cryptography** option under the **Advanced** tab.



☑ Activate link at start

□ HPR support

☑ APPN support

□ Auto-activate support

□ Link to preferred NN server

□ Solicit SSCP sessions

☑ Use cryptography

PU name:

Maximum PIU size: 32767

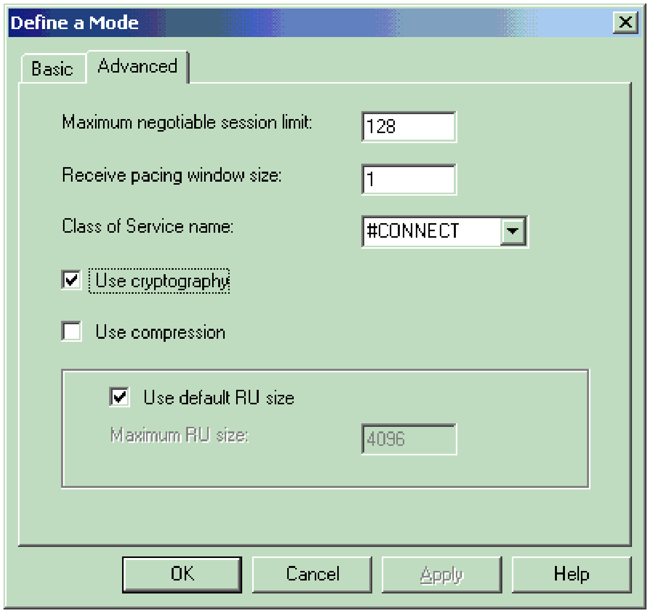
Local Node ID

Block ID: 05D

Physical Unit ID: 00000

Figure 25-20 Enabling cryptography for a LAN connection

For LU 6.2, a mode has to be defined with **Use Cryptography** under the **Advanced** tab. That mode has to be used while connecting to the peer LU.



Define a Mode

Maximum negotiable session limit: 128

Receive pacing window size: 1

Class of Service name: #CONNECT

☑ Use cryptography

□ Use compression

☑ Use default RU size

Maximum RU size: 4096

Figure 25-21 Enabling cryptography in a Mode configuration to be used in LU6.2

25.10.5 Tracing cryptography functionality

AMDSEC provides tracing through the **`amdsec trace`** command option. For taking the traces follow these steps:

1. To start tracing, issue the command **`amdsec trace on`** from the command prompt.
2. To stop tracing, issue the command **`amdsec trace off`** from the command prompt.
3. Copy the collected trace to a file using **`amdsec trace copy <trace-file>`** command.
4. To format the trace file into a readable format, use **`amdfmt <trace-file>`**. The formatted output is shown in the command window itself. To store the formatted output in a file, use the redirection operator so that the formatted output will be stored in a file named formattedtracefile. For example:

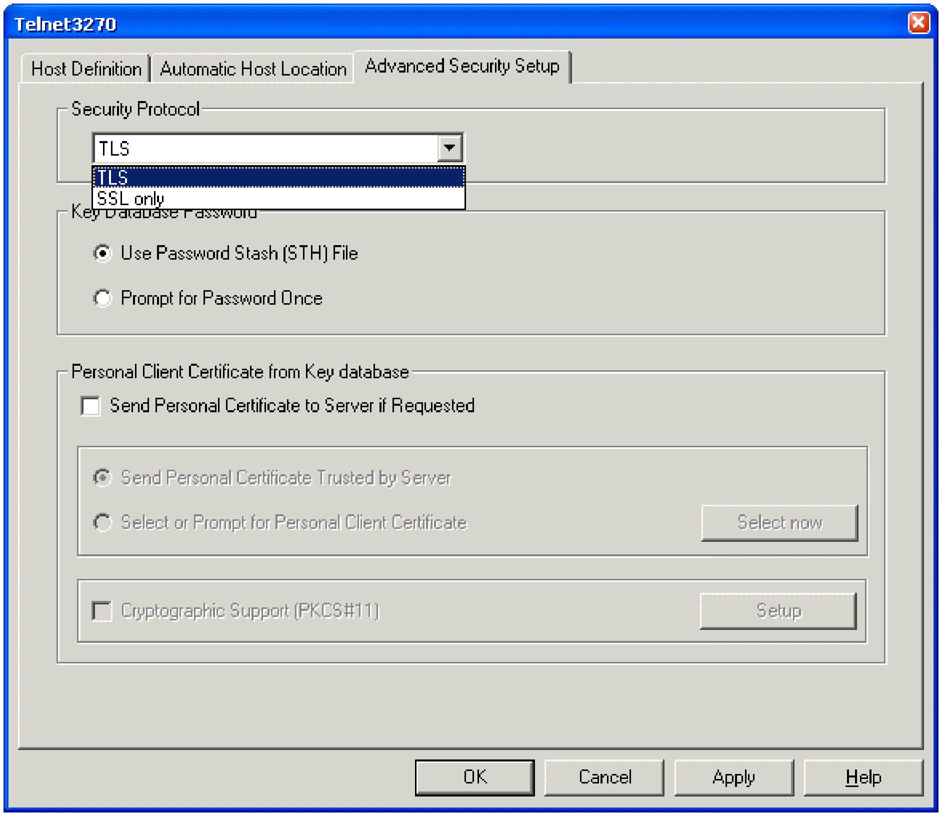
```
amdfmt mytrcfile > formattedtracefile
```

25.11 Transport Layer Security protocol support

Personal Communications Version 5.7 supports the Transport Layer Security (TLS) protocol for secure encryption and authentication. TLS is the IETF supported version of Secure Sockets Layer (SSL) protocol. The difference between SSL and TLS are cosmetic in nature. More details about the TLS protocol can be found at:

http://www.ietf.org/rfc/rfc2246.txt

Users can select if they want the client to start negotiating with TLS or SSL protocol. If the host does not support TLS protocol, then the client will automatically use the SSL protocol. The user can select the protocol from the advanced security tab of the Telnet configuration. See Figure 25-22.



Telnet3270

Security Protocol: TLS

TLS
SSL only

Key Database Password

● Use Password Stash (STH) File

○ Prompt for Password Once

Personal Client Certificate from Key database

□ Send Personal Certificate to Server if Requested

● Send Personal Certificate Trusted by Server

○ Select or Prompt for Personal Client Certificate

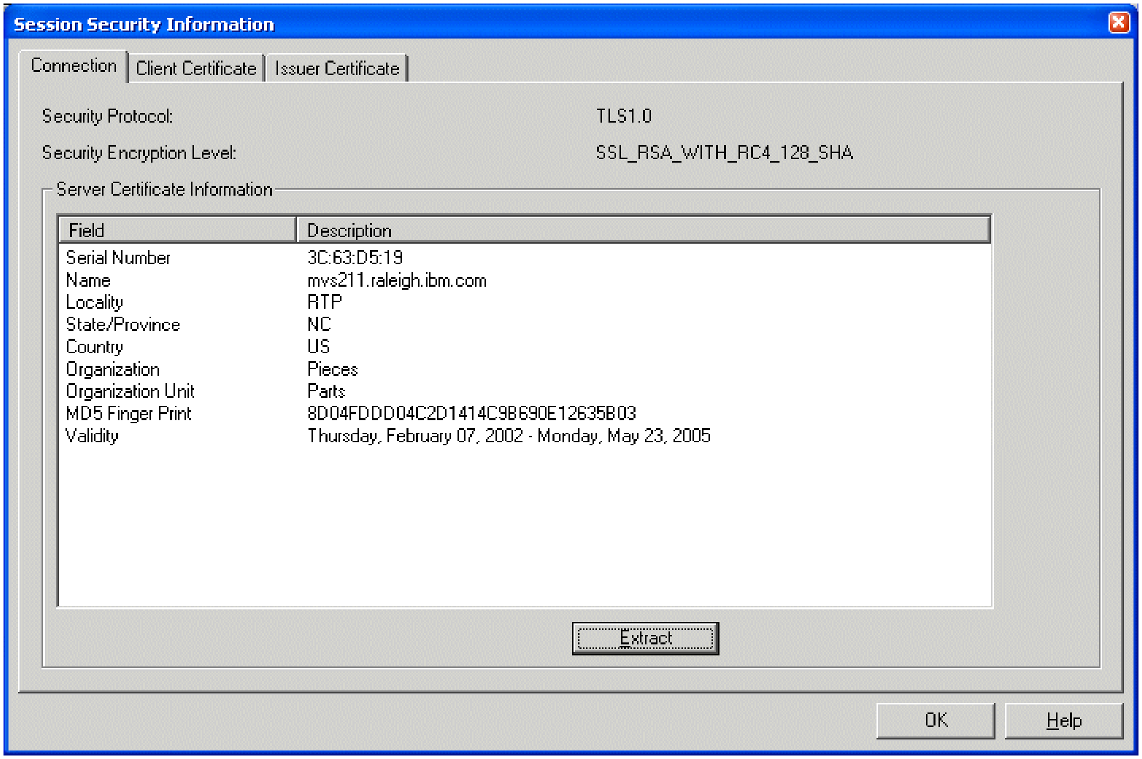
□ Cryptographic Support (PKCS#11)

Figure 25-22 Selecting the protocol to be used

The default is TLS protocol.

When one connects to the host and the communication fails, the error code is displayed in the status bar. The status bar history help now has explanations for all the error codes that appear in the status bar. The **Communication -> Security Information** dialog displays the security information pertinent to the connection.

The dialog displays the certificate the server sent to the client, the issuer certificate details; and if client authentication was performed, the certificate which the client sent to the server.



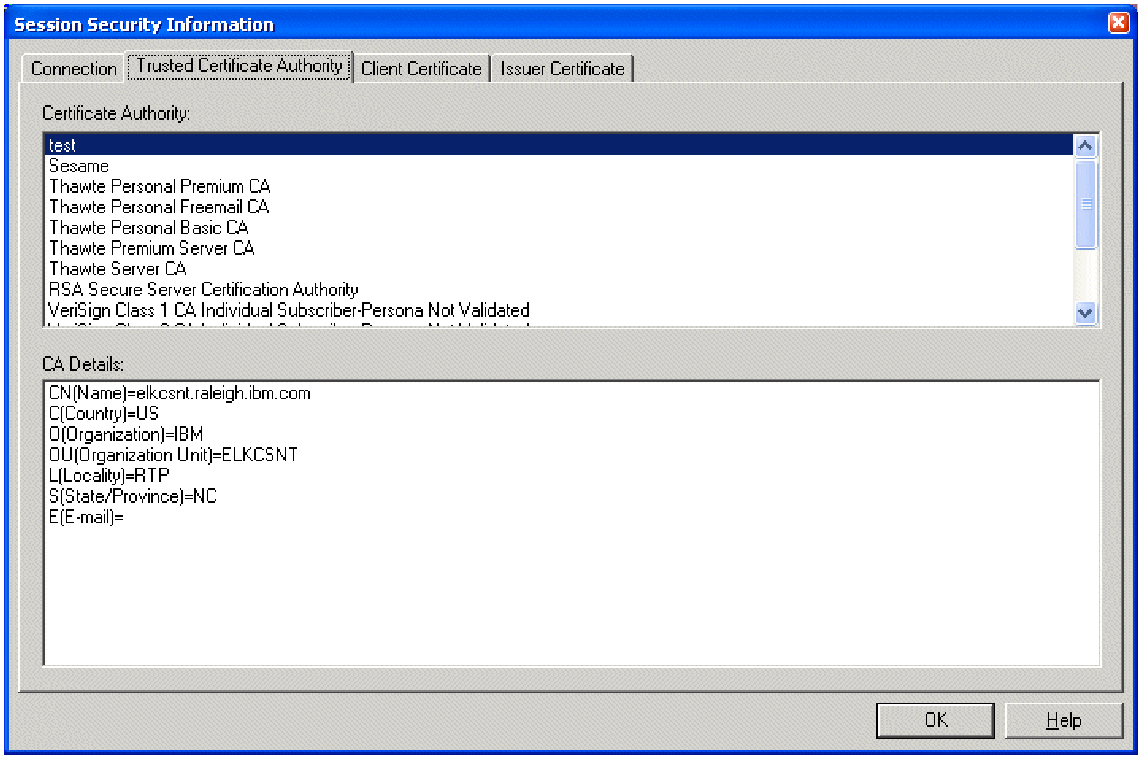
Security Protocol: TLS1.0

Security Encryption Level: SSL_RSA_WITH_RC4_128_SHA

Field	Description
Serial Number	3C:63:D5:19
Name	mvs211.raleigh.ibm.com
Locality	RTP
State/Province	NC
Country	US
Organization	Pieces
Organization Unit	Parts
MD5 Finger Print	8D04FDDD04C2D1414C9B690E12635B03
Validity	Thursday, February 07, 2002 - Monday, May 23, 2005

Figure 25-23 The security information dialog

Also, the server certificate can be extracted and saved to a file. If the key database was opened with a password (that is, in the **Advanced Security Setup** page of the Telnet configuration dialog, the **key database password** was selected to be **Prompt for password once)**, then an extra tab page is displayed. The tab contains the list of certificate authorities that the client trusts. See Figure 25-23.



Certificate Authority:

test
Sesame
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
RSA Secure Server Certification Authority
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

CA Details:

CN(Name)=elkcsnt.raleigh.ibm.com
C(Country)=US
O(Organization)=IBM
OU(Organization Unit)=ELKCSNT
L(Locality)=RTP
S(State/Province)=NC
E(E-mail)=

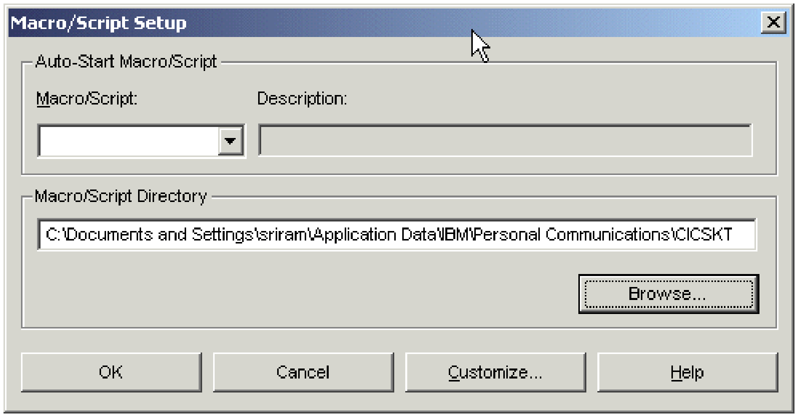
Figure 25-24 The trusted Certificate Authority List

If the secure connection failed but the server sent the certificate to Personal Communications, the security information panel displays the certificate sent by the server. This can be useful in finding out why the connection failed. If the server did not send the certificate or if Personal Communications cannot open the local keyring or some other fatal error occurred, then the panel will not be displayed and the menu item **Communication -> Security Information** will be disabled.

25.12 Macro enhancements

In previous versions of Personal Communications, there was only one location where macros were stored so that the emulator could use them (for display while playing, using EHLLAPI, for autostart macros). The one location was the data directory location (classic private, all users, or per user), which is selected during the installation. This tends to be limiting in cases where users want a better structure for storing the macro files. Personal Communications now supports an additional macro directory that can be specified for each session. The macros will be listed from the data directory and the newly listed directory.

The session specific directory for macros can now be specified at **Edit -> Preferences -> Macro/Script Setup**. By default, this field is empty.



C:\Documents and Settings\sriram\Application Data\IBM\Personal Communications\CICSKT

Figure 25-25 Setting the session specific Macro Directory

On setting this directory, macros for listing will now be picked up from the specified directory and the data directory. Also, this new directory becomes the default Save directory location when one records and macro. If there are two macro's of the same name in both the session-specific macro/script directory, and the application data directory, then the macro in the session specific macro/script directory will be listed.

As an example, let us say a user wants to use three different host applications (TSO1, CICSKT and IMS™) and has configured three session profiles to connect to the applications. Also, let us assume that the user has ten macros per application to do specific tasks (thirty in total) and five macros that are used across all applications.

In the previous releases, all the 35 macros are listed when the user wanted to play a macro. Also, if there were macros performing a similar task like logon, but were specific to the application, the macros had to be uniquely named (like TSO1_Logon.mac,CICKT_Logon.mac and IMS_Logon.mac).

With the new feature, the user can store the ten macros in three different directories (one for each application) and set them to the respective profile. The five common macros will reside in the data directory. Now, whenever the user is in any session and needs to play a macro, only fifteen macros will be listed. Also, the users can have the same names for macros that perform similar tasks if they are stored in different directories. Now the user has a session specific list of macros, and selecting the macros to play is much simpler and specific.

There is also an option that allows one extra global directory similar to the application data directory. This can be set from the User Preferences manager Macro/Script directory. All the macros present in this directory will be listed in addition to the session specific macro directory and the data directory. This can be useful in a setup where the administrator wants a set of macros to be shared across users. The administrator can set this directory with macros in a network mapped drive, and have all the users point to this network drive. Also, in Windows 2000 and above where there can be multiple users who use the same machine, if the application data directory is per user, then this option can be used to shared macro's across users.

With macros being stored in three directories, there is a possibility of a name clash while listing if multiple macro's have the same name. If there are multiple macro's with the same name, PCOMM will list the first macro it finds in precedence order of directories. The precedence order is:

- Session specific macro directory (specified in **Edit -> Preferences -> Macro/Script**)
- Application data directory (Classic private, All user or All User)
- The global Macro script directory (specified in User preferences manager)

Important: This feature is available in Personal Communications Version 5.7 CSD1 and above only.

26

Migration

Personal Communications Version 5.7 can be installed over all previous versions of Personal Communications beginning with V4.3. During the installation process the older version will be detected and uninstalled before the installation of Personal Communications Version 5.7 begins. The uninstall process only uninstalls the product itself. Therefore, any user data and configuration files (for example the `\private` subdirectory) will not be deleted.

In releases of Personal Communications prior to V5.5, all configuration files, macros and other client customization files were located in the `\private` subdirectory.

Personal Communications V5.5 allowed users to store application data either in the classic `\private` subdirectory or in subdirectories as shown in Table 26-1 on page 954. When installing Personal Communications Version 5.7, it will detect the location of the data for the previous version. It will copy that data to the new Application Data Location as specified for the new installation of Personal Communications Version 5.7.

26.1 Migration during installation

Personal Communications allows you to customize the automatic migration process when updating from previous versions of Personal Communications. Migration is optional, but when selected, all profile references are updated to the current path for profiles selected at installation time that are moved during automatic migration. For more details on locations of application data of Personal Communications please refer to table in online documentation *Personal Communications for Windows, Version 5.7: CD-ROM Guide to Installation*, GC31-8079-08, "Chapter 3."

If the **User's Application Data Folder** is selected, the profile paths shown in Table 26-1 are used.

Table 26-1 Application data location, UserProfile

Operating System	User Class Directory (Current User)	System Class Directory
Windows 95/98/Me	C:\Windows\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\PersonalCommunications
Windows 95/98/Me (user profiles enabled)	C:\Windows\Profiles\%USERNAME%\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows NT 4.0	C:\Winnt\Profiles\%USERNAME%\Application Data\IBM\Personal Communications	C:\Winnt\Profiles\All Users\Application Data\IBM\Personal Communications
Windows 2000 / XP	C:\Documents and Settings\%USERNAME%\Application Data\IBM\Personal Communications	C:\Documents and Settings\All Users\Application Data\IBM\Personal Communications

If the **All Users Common Application Data Folder** is selected, the profile paths shown in Table 26-2 are used.

Table 26-2 Application data location, AllUsers

Operating System	User Class Directory (Current User)	System Class Directory
Windows 95/98/Me	C:\Windows\All Users\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows 95/98/Me (user profiles enabled)	C:\Windows\All Users\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows NT 4.0	C:\Winnt\Profiles\All Users\Application Data\IBM\Personal Communications	C:\Winnt\Profiles\All Users\Application Data\IBM\Personal Communications

Operating System	User Class Directory (Current User)	System Class Directory
Windows 2000 / XP	C:\Documents and Settings\All Users\Application Data\IBM\Personal Communications	C:\Documents and Settings\All Users\Application Data\IBM\Personal Communications

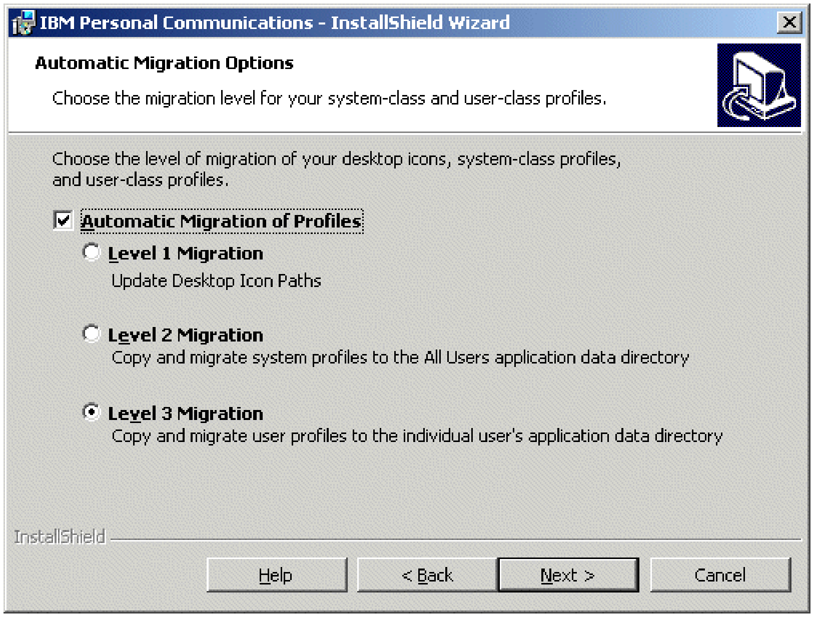
> **Note:** In Microsoft Windows 95, 98, and Me, you have the option of enabling user profiles. A user profile is an account maintained by the operating system that keeps track of a particular user's files and system configuration. When a user logs on to the system, Windows is loaded with the logged-on user's files and system configuration settings in place. In Windows NT, 2000, and XP, user profiles are always enabled.

If **Classic Private Directory** is selected, the profile paths shown in Table 26-3 are used.

Table 26-3 Application data location, Private directory

Operating System	User Class Directory (Current User). Notes:1,2	System Class Directory
Windows 95/98/Me	C:\Program Files\IBM\Personal Communications\Private	C:\Program Files\IBM\Personal Communications\Private
Windows 95/98/Me (user profiles enabled)	C:\Program Files\IBM\Personal Communications\Private	C:\Program Files\IBM\Personal Communications\Private
Windows NT 4.0	C:\Program Files\IBM\Personal Communications\Private	C:\Program Files\IBM\Personal Communications\Private
Windows 2000 / XP	C:\ Program Files\IBM\Personal Communications\Private	C:\ Program Files\IBM\Personal Communications\Private
Note1: If the User Preference Manager (UPM) was set to a directory other than the default directory, Personal Communications will utilize that directory to store the user–class files. System–class files are always stored in the Private directory. Note2: For the classic Private directory locations, C:\Program Files\IBM\ Personal Communications is the drive where Personal Communications is installed		

If the user is doing a custom installation, the window shown in Figure 26-1 will be provided to change the level of migration performed, ranging from no migration to full migration. A typical installation will result in a full migration.



Automatic Migration Options

Choose the migration level for your system-class and user-class profiles.

Choose the level of migration of your desktop icons, system-class profiles, and user-class profiles.

☑ Automatic Migration of Profiles

○ Level 1 Migration
Update Desktop Icon Paths

○ Level 2 Migration
Copy and migrate system profiles to the All Users application data directory

● Level 3 Migration
Copy and migrate user profiles to the individual user's application data directory

Figure 26-1 Migration levels

The levels of migration vary based on the location of the application data that the installer has chosen.

- Level 1 Migration

  Only desktop icons are migrated.

- Level 2 Migration

  This is considered system-level migration. It includes desktop icons and adds system-class profiles. Table 26-4 describes the system-class files that will be migrated.

Table 26-4 System-class profile file extensions

File extension	File type
.acg	SNA configuration
.mlg	Default message log
.trc	Unformatted trace
.tlg	Formatted trace

Level 2 also migrates user-class profiles when migrating profiles to either All Users Common Application Data Folder or the Classic Private Directory. For a list of user-class profile files, see Table 26-5.

Table 26-5 User-class profile file extensions

File extension	File type
.ws	Workstation profile
.bch	Multiple sessions
.ini	Session size and location
.pmp	Popup-keypad configuration
.kmp	Keyboard configuration
.srl	File transfer list
.ndc	AS/400 connection configuration
.upr	AS/400 user profile
.tto	AS/400 data transfer request (receive)
.tfr	AS/400 data transfer request (send)
.bar	Toolbar setup
.mac	Macro
.mmp	Mouse setup
.xlt	Translation table
.xld	DBCS translation table
.cert	Certificate
.sth	Password stach
.adu	Automatic dial utility
.kbd	Certificate Management database
.der	Binary DER

- Level 3 migration

  This is considered a full migration. It includes desktop icons, system-class profiles (Table 26-4), and user-class profiles (Table 26-5).

It is recommended that an individual user accept the automatic migration option selected, and that only Personal Communications Version 5.7 administrators use the different levels of migration.

In previous releases of Personal Communications, all of the user data migration occurred during the reboot of the machine after the install was run. In this release, the system-class profiles are moved and migrated during the first reboot after Personal Communications Version 5.7 is installed. The desktop icons and user-class profiles are moved and migrated the first time a user logs on after Personal Communications Version 5.7 is installed.

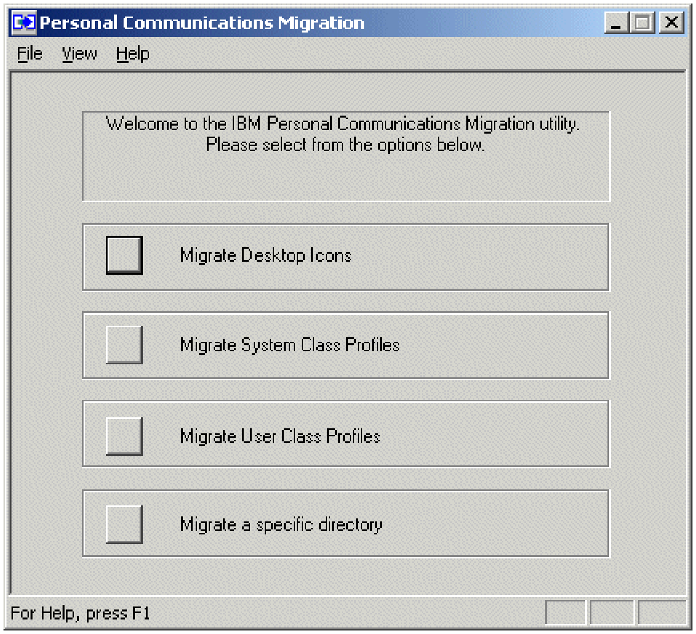
A log is created during the migrations. This log file is named `pcsmig.log` and is located in the system level profile directory. This log file will contain a history of what was migrated and what files were moved, including their original and new locations. This file is essential in finding any problems that occurred during the migration. If a user has migration problems, or any problems with his profiles after Personal Communications Version 5.7 is upgraded, this `pcsmig.log` file may be required for problem determination. The `pcsmig.log` file is also written during a manual migration.

26.2 Migration Utility

This migration process can be run manually after Personal Communications Version 5.7 has been installed. The Migration Utility is used to copy the configuration files for Personal Communications V5.6 by reading the information stored in configuration files from previous versions of Personal Communications. This process allows you to avoid having to re-enter all of your configuration data when you upgrade to Personal Communications Version 5.7.

Start the Migration Utility by clicking **Start -> Programs -> IBM Personal Communications -> Administration and PD -> Migration Utility**.

The resulting window is shown in Figure 26-2.


Personal Communications Migration
File
View
Help
Migrate Desktop Icons
Migrate System Class Profiles
Migrate User Class Profiles
Migrate a specific directory

Welcome to the IBM Personal Communications Migration utility.
Please select from the options below.

For Help, press F1

Figure 26-2 Migration Utility

If you do not see your session profiles in the session manager window after migration, your old session definitions etc. might be in a subdirectory that the new Personal Communications has not recognized. In that case, click the button **Migrate a specific directory**.

See the panel in Figure 26-3 to choose the subdirectory from.

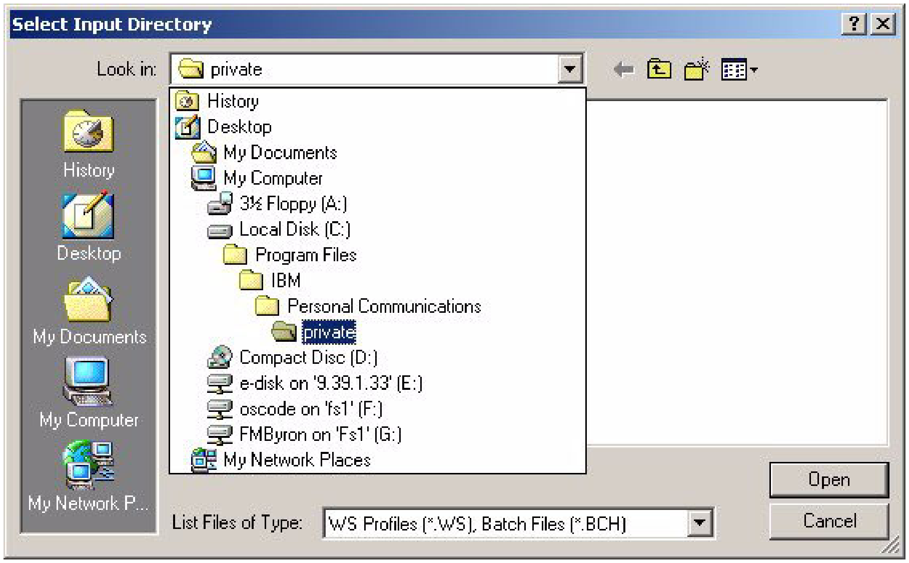


Figure 26-3 Select specific directory for migration

In previous releases of Personal Communications, there have been small changes in the workstation profiles (.ws) from one release to another. Personal Communications just executes, expecting the profile contains the keywords as recognized by this latest version of Personal Communications.

For the future, Personal Communications has added a version number to the Personal Communications profile to allow it to differentiate among different versions of the profiles. The keyword is in the `[Profile]` section and is named `Version`. If this keyword does not exist in a profile, the profile is from Personal Communications 5.0 or earlier.

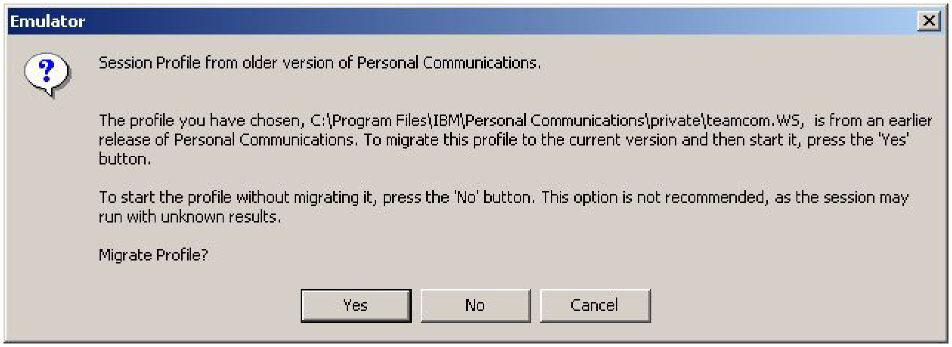
All profiles from Personal Communications V5.5 have a version number of 5. The profile version number does not correlate to the Personal Communications version number.

Example 26-1 Version number in .ws file

```
[Profile]
ID=WS
Version=5
[Telnet3270]
HostName=9.39.1.37
HostPortNumber=23
Security=N
[Communication]
```

```
Link=telnet3270
[3270]
QueryReplyMode=Auto
HostCodePage=1047-U
```

If a user starts a Personal Communications profile from a previous release of Personal Communications, the user will be prompted to migrate the profile to the current version as shown in Figure 26-4.



Session Profile from older version of Personal Communications.

The profile you have chosen, C:\Program Files\IBM\Personal Communications\private\teamcom.WS, is from an earlier release of Personal Communications. To migrate this profile to the current version and then start it, press the 'Yes' button.

To start the profile without migrating it, press the 'No' button. This option is not recommended, as the session may run with unknown results.

Migrate Profile?

Figure 26-4 Prompt for migrating down level profile

Whenever any profile is modified, its version number will be incremented by one.

Example 26-2 Version number in migrated .ws file

```
[Profile]
ID=WS
Version=6
[Telnet3270
....
```

There is also an option letting the user run the profile as is; however, it is not recommended to run the profile as is.

If a user starts a profile created in a newer version of Personal Communications than he has installed on his machine, Personal Communications will display a pop-up window telling the user that the profile is from a new release, and that the user must upgrade the version of Personal Communications if the profile is run.

27

Security

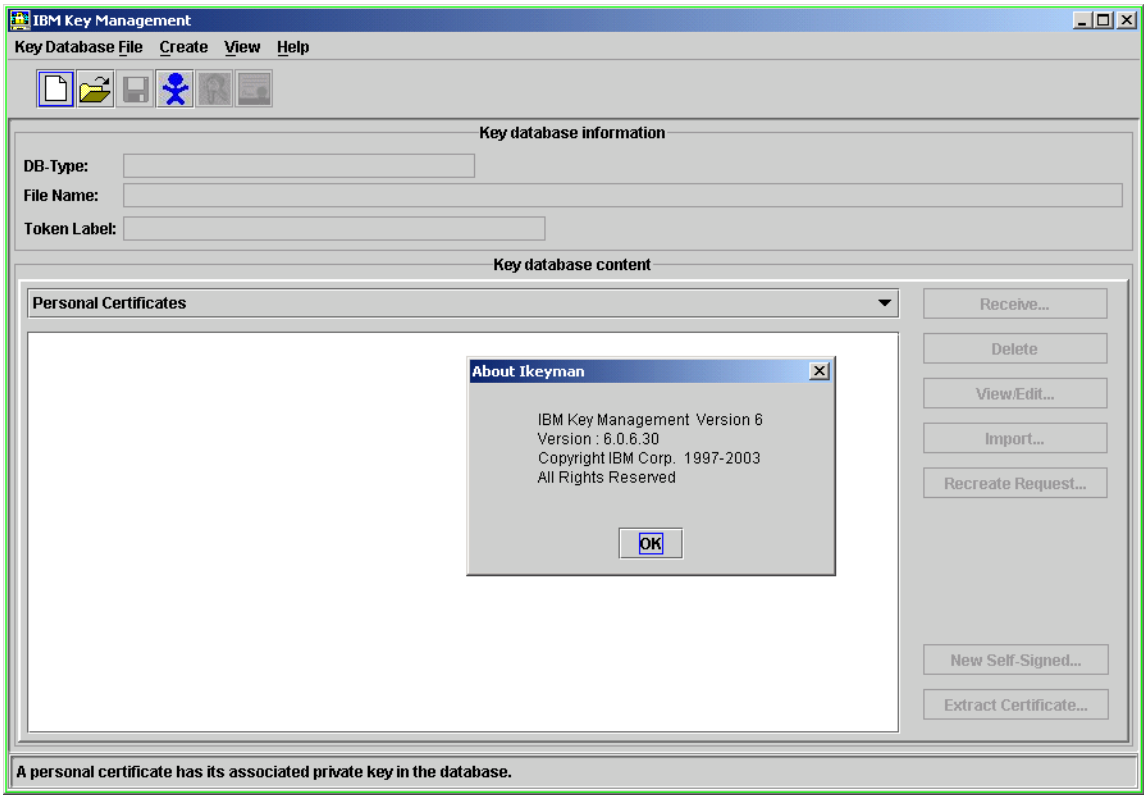
Personal Communications Version 5.7 supports the industry-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocol to insure privacy of data transmission. For an overview of the operation of SSL and TLS, refer to “Secure Sockets Layer” on page 1038.

27.1 Enhancements in certificate management

Personal Communications includes GSKit Version 6 (Global Security Toolkit) for certificate management.

You can use it through the command line interface `ikeyman`, the Certificate Wizard, or the certificate management utility.

To start the certificate management utility click **Start -> Programs -> Personal Communications -> Utilities -> Certificate Management**. Figure 27-1 shows the version of the key management, which appears when you click **Help -> About**.



IBM Key Management Version 6
Version : 6.0.6.30
Copyright IBM Corp. 1997-2003
All Rights Reserved

A personal certificate has its associated private key in the database.

Figure 27-1 certificate management utility with key management version

The enhancements over previous versions as contained in Personal Communications and Host On-Demand are:

- A wider range of formats for certificate file as shown in Figure 27-2 (Crytographic Token is a device or smart card holding the certificate).

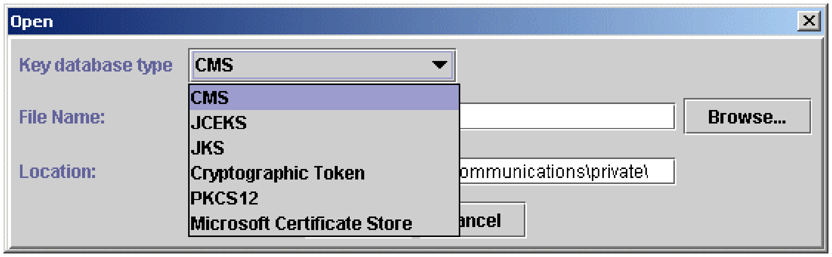


Figure 27-2 Formats of certificate files

- Extend supported types of key databases.

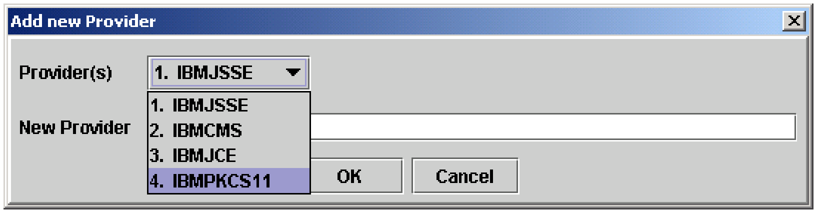


Figure 27-3 Selection of providers for key database file types

27.1.1 Example of certificate management

The use of `ikeyman` is well described in the online documentation. Experience shows that for Personal Communications, the GUI Certificate Management Utility is preferred. So we will use the certificate management utility GUI for our example. To show a general use of the certificate management utility, we will set up a scenario where we have the Host On-Demand Redirector being used as a proxy for a Personal Communications secure Telnet session.

The procedure to install a certificate is the same as far as Personal Communication and its certificate management utility are concerned, if the certificate was created at another source (for example, at a zSeries Telnet server).

Also, the procedure of creating a self signed certificate using Host On-Demand certificate management utility applies as well to create a self signed certificate using the GSKit V6 certificate management utility of Personal Communications.

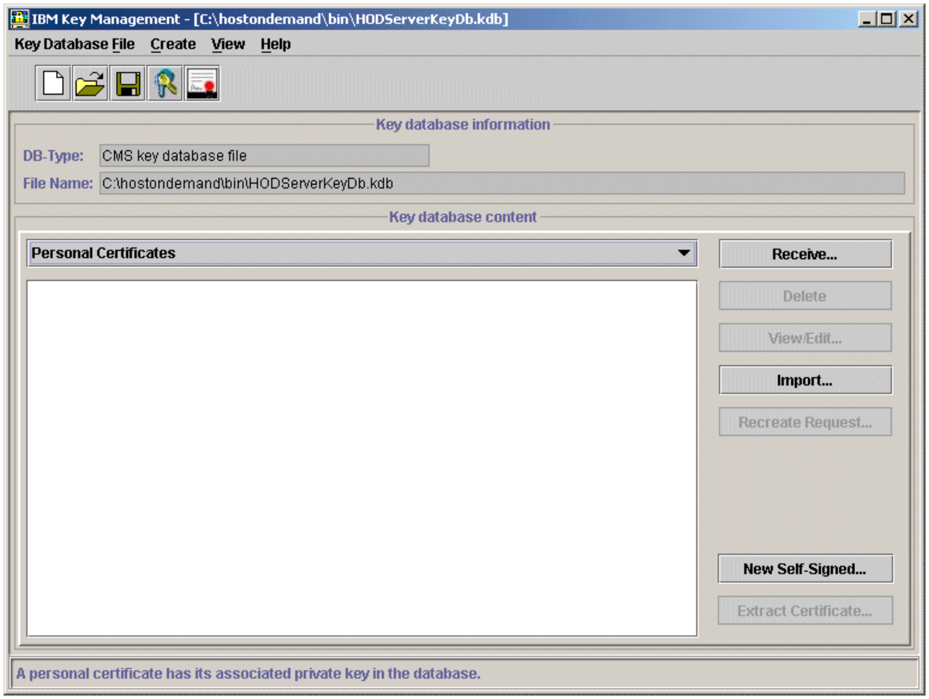
Here are the steps for our example:

1. Use Host On-Demand certificate management utility to issue a self signed certificate which is added into Host On-Demand key database.
2. Extract the certificate from the Host On-Demand key database as ARM file for use in Personal Communications.
3. Set up Host On-Demand Redirector with client side security and restart it to pick up the configuration change and the certificate.
4. Import the certificate into the key database of Personal Communications Version 5.7.
5. Setup a 3270 Telnet session with Personal Communications Version 5.7 to use SSL with certificate.

Creating a certificate using HOD certificate management utility

We use the Host On-Demand certificate management utility to create a new self signed certificate as follows:

Open Host On-Demand Key Management and select the **Personal Certificates** from the drop down box. You will see Figure 27-4.



IBM Key Management - [C:\hostondemand\bin\HODServerKeyDb.kdb]

Key database information

DB-Type: CMS key database file

File Name: C:\hostondemand\bin\HODServerKeyDb.kdb

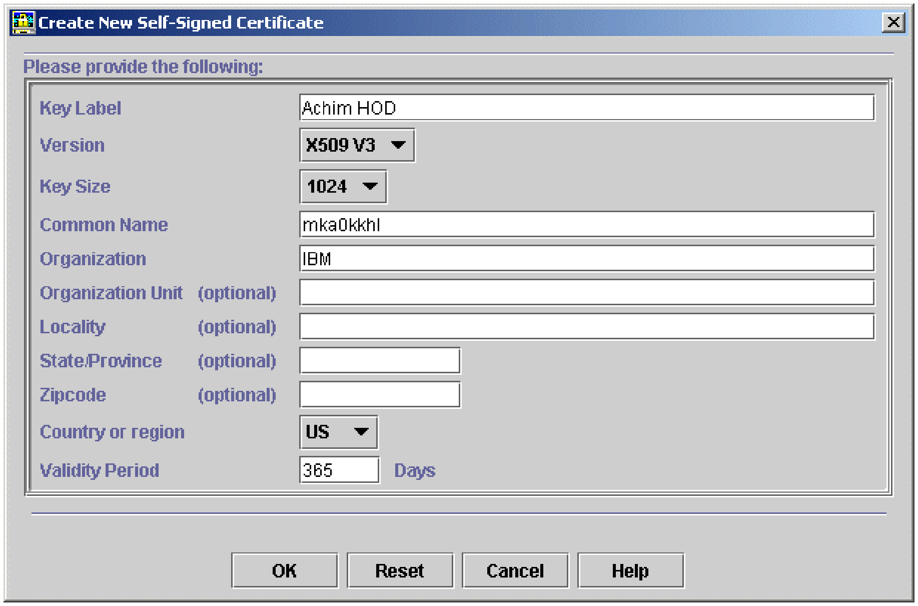
Key database content

Personal Certificates

A personal certificate has its associated private key in the database.

Figure 27-4 Key Management of Host On-Demand

Click **New Self Signed**. You will get the window as shown in Figure 27-5.



Create New Self-Signed Certificate

Please provide the following:

Key Label	Achim HOD
Version	X509 V3
Key Size	1024
Common Name	mka0kkhl
Organization	IBM
Organization Unit (optional)	
Locality (optional)	
State/Province (optional)	
Zipcode (optional)	
Country or region	US
Validity Period	365 Days

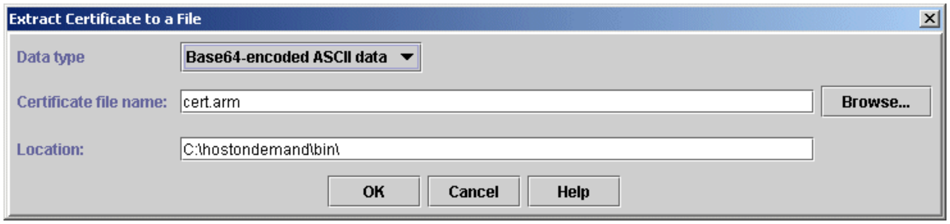
Figure 27-5 Create new self signed certificate

Fill in a key label and the organization. The rest of the field have been left to their default values. This includes the Common Name, which is the same as found by clicking **My Computer -> Properties -> Network Identification -> Full Computer Name**.

After clicking **OK,** this certificate is added to your Personal Certificates.

Extracting a Certificate

We now need to extract the certificate that is currently contained in our key database file. For Personal Communications we need to extract it as a Base 64 encoded ASCII file. To create that file we click **Extract** and receive the panel as shown in Figure 27-6. Using **Browse** we select the subdirectory to save the certificate.



Data type: Base64-encoded ASCII data

Certificate file name: cert.arm

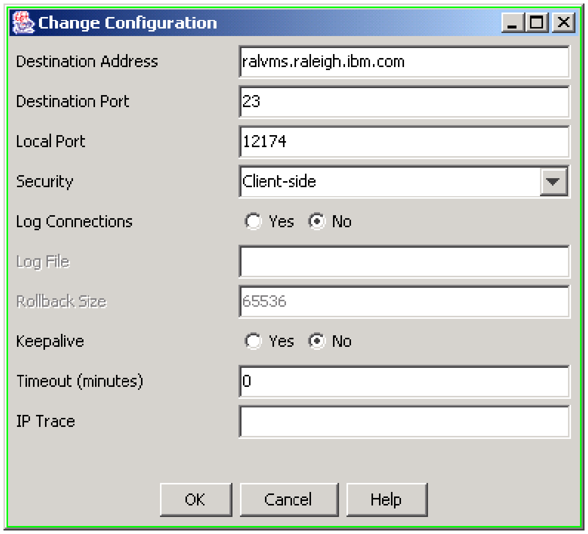
Location: C:\hostondemand\bin\

Figure 27-6 Extracting certificate from key database

Click **OK** and we are done, extracting a self signed certificate from our Host On-Demand key database so that it can be used by Personal Communications. We end the Host On-Demand key database management utility.

Setting up HOD Redirector for secure session with Telnet client

See Chapter 7.3.1, “Configuring the Redirector” on page 340 for the general procedure how to set up the Redirector. For our example in Figure 27-7, we use a client-side security.



Destination Address	ralvms.raleigh.ibm.com
Destination Port	23
Local Port	12174
Security	Client-side
Log Connections	○ Yes ● No
Log File	
Rollback Size	65536
Keepalive	○ Yes ● No
Timeout (minutes)	0
IP Trace	

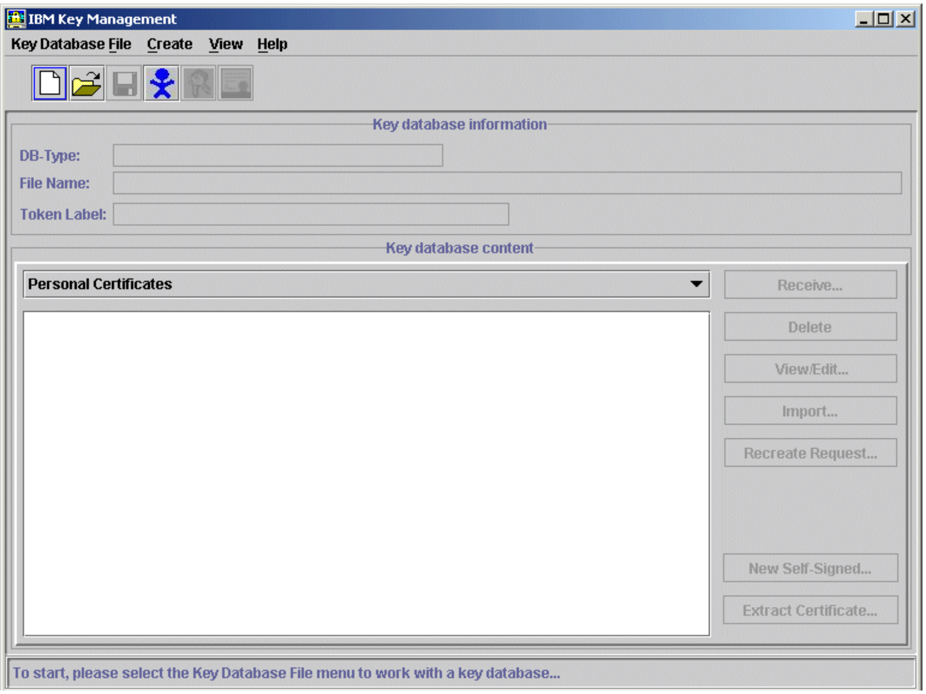
Figure 27-7 Setting up Redirector for client -side security

Note: Be sure to stop and restart the Redirector so it picks up the new definitions.

You need to restart it also when changing certificates!

Setting up Personal Communications for secure session

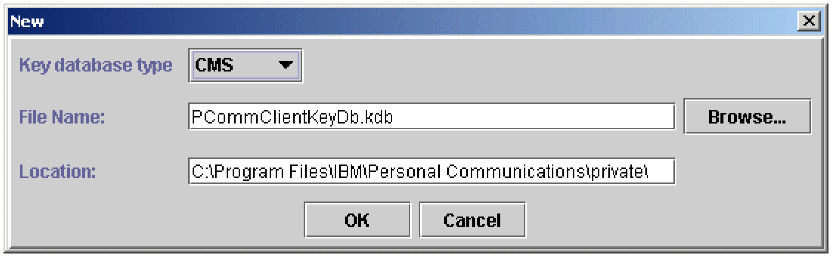
We use the Key database management of Personal Communications to implement the Host On-Demand certificate into the key database of Personal Communication. Click **Start -> Programs -> IBM Personal Communications -> Utilities -> Certificate Management**. The following window is displayed.



To start, please select the Key Database File menu to work with a key database...

Figure 27-8 Key Management of Personal Communications

In Key Management of Personal Communications as shown in Figure 27-8, we click **Key database file -> New** to create a new key ring database file. The type has to be CMS as shown in example of Figure 27-9.



New

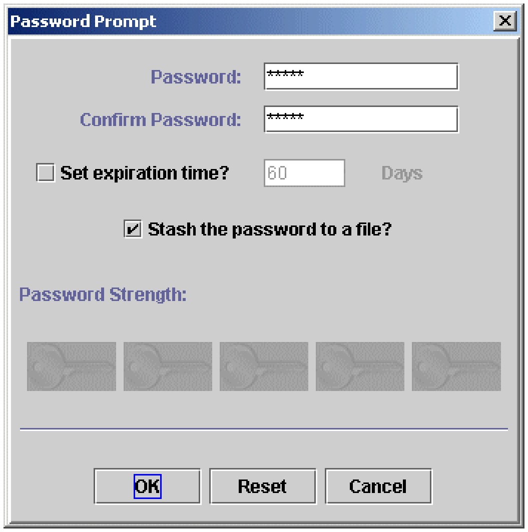
Key database type: CMS

File Name: PCommClientKeyDb.kdb

Location: C:\Program Files\IBM\Personal Communications\private\

Figure 27-9 Opening key database file and select type

We use the default password `pcomm` and select **Stash password to a file** as shown in Figure 27-10.



Password Prompt

Password: *****

Confirm Password: *****

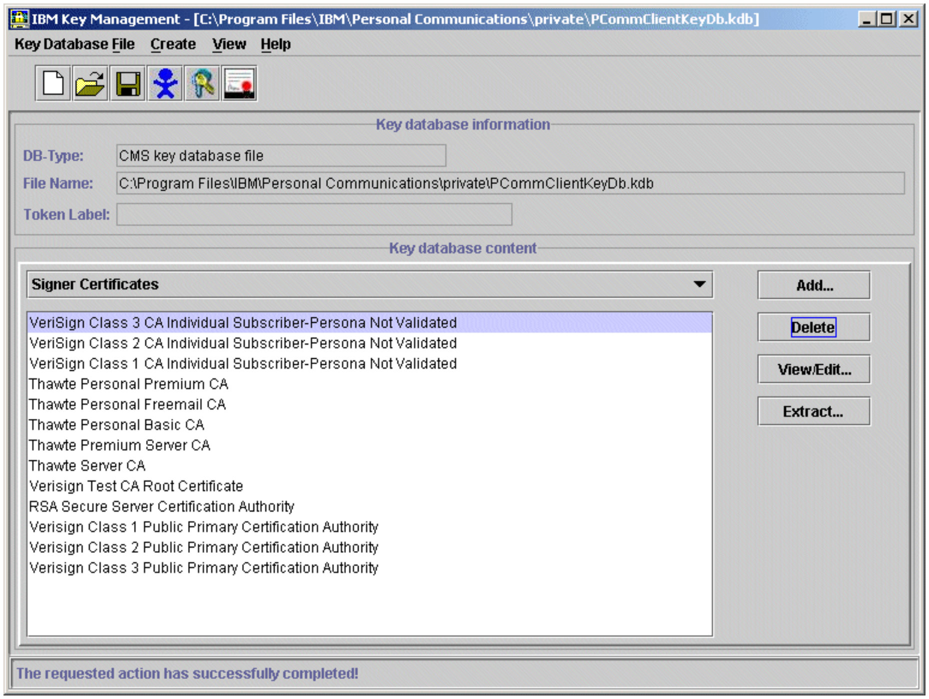
□ Set expiration time? 60 Days

☑ Stash the password to a file?

Password Strength:

Figure 27-10 Password prompt and stash password to file

We now see the Signer Certificates as shown in Figure 27-11.



IBM Key Management - [C:\Program Files\IBM\Personal Communications\private\PCommClientKeyDb.kdb]

Key database information

DB-Type: CMS key database file

File Name: C:\Program Files\IBM\Personal Communications\private\PCommClientKeyDb.kdb

Token Label:

Key database content

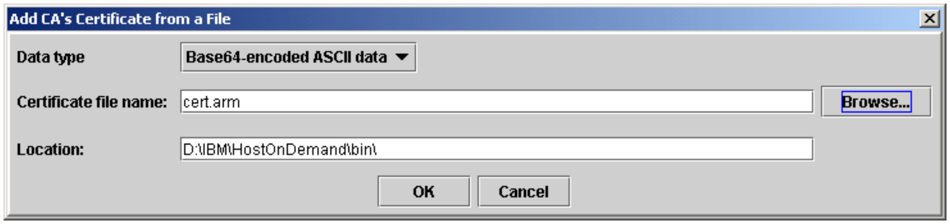
Signer Certificates

VeriSign Class 3 CA Individual Subscriber-Persona Not Validated
VeriSign Class 2 CA Individual Subscriber-Persona Not Validated
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
Verisign Test CA Root Certificate
RSA Secure Server Certification Authority
Verisign Class 1 Public Primary Certification Authority
Verisign Class 2 Public Primary Certification Authority
Verisign Class 3 Public Primary Certification Authority

The requested action has successfully completed!

Figure 27-11 Signer Certifications pane in GSKit6 window

We now select **Add** to add the certificate created previously on the Host On-Demand server. On the Host On-Demand server, we extracted the ARM file, Base64 encoded ASCII, which we now need for Personal Communications. Use the **Browse** button to point to the location of that file. In the example for taking our screen copies Host On-Demand and Personal Communications on the same machine, so we find the certificate on the default Host On-Demand subdirectory as shown in Figure 27-12.



Add CA's Certificate from a File

Data type: Base64-encoded ASCII data

Certificate file name: cert.arm

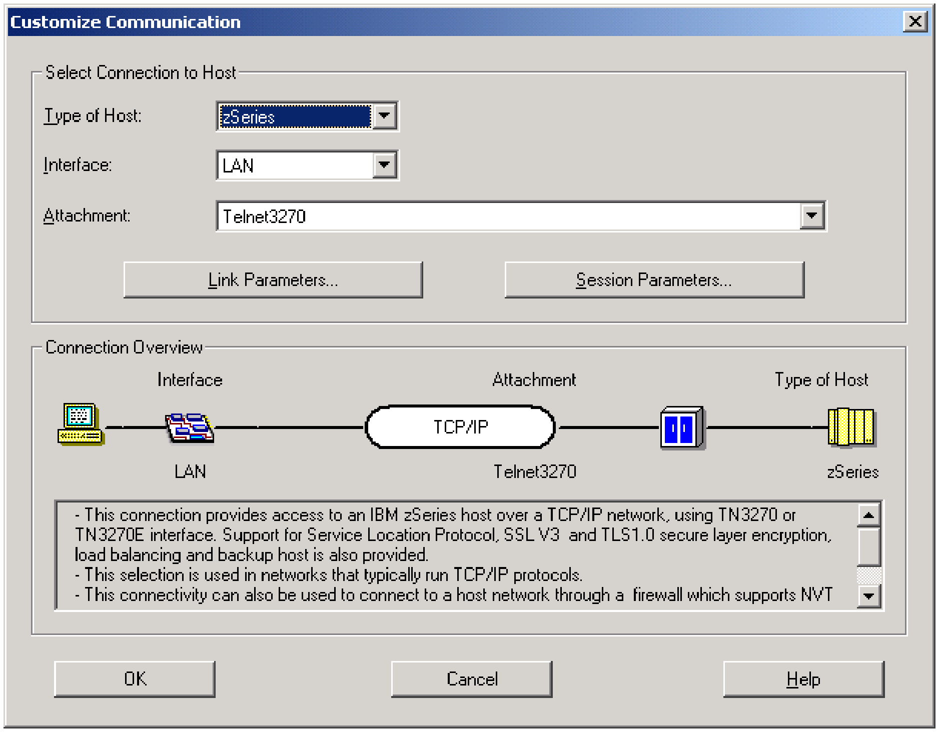
Location: D:\IBM\HostOnDemand\bin\

Figure 27-12 Adding a certificate for Personal Communications

After clicking **OK**, we are prompted to enter a label for the new certificate. Choose any which you can remember. Click **OK** and the new certificate is included in the list of Signers Certificates.

Now we can close the certificate management. We open the session manager of Personal Communications by clicking **Start -> Programs -> Personal Communications -> Start or configure Sessions**.

We click **New** and receive the session configuration window of Personal Communications.



Type of Host: zSeries

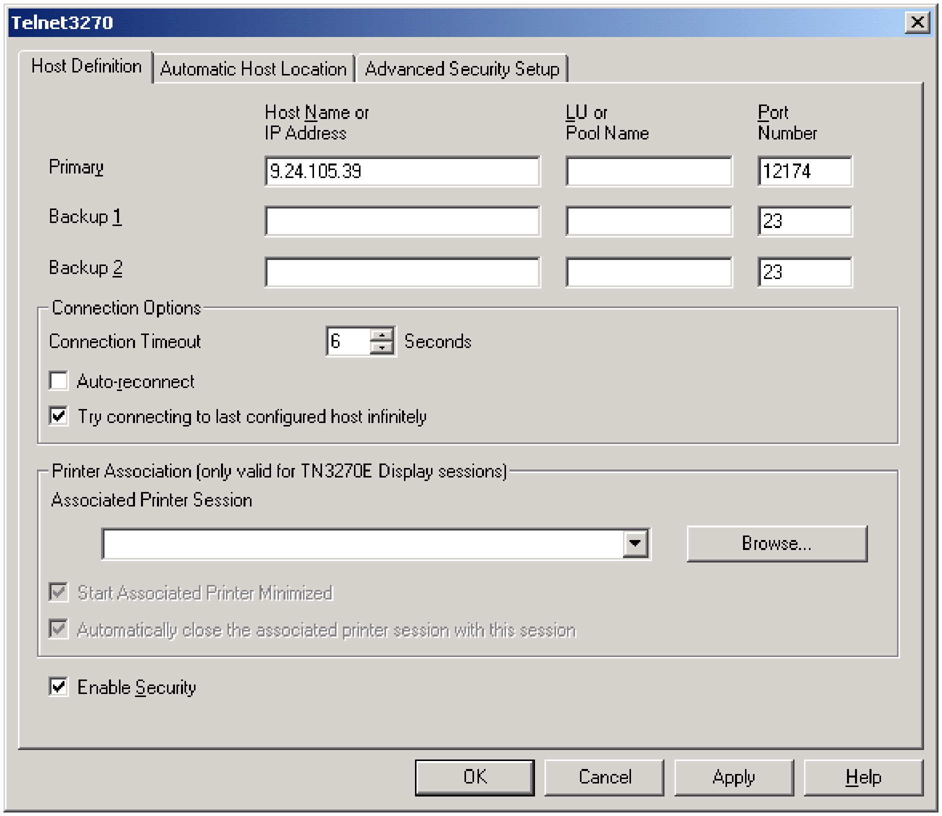
Interface: LAN

Attachment: Telnet3270

- This connection provides access to an IBM zSeries host over a TCP/IP network, using TN3270 or TN3270E interface. Support for Service Location Protocol, SSL V3 and TLS1.0 secure layer encryption, load balancing and backup host is also provided.
- This selection is used in networks that typically run TCP/IP protocols.
- This connectivity can also be used to connect to a host network through a firewall which supports NVT

Figure 27-13 Telnet configuration

The window defaults to a Telnet configuration. We click **Link Parameters** and for the window to enter the IP address and port, and to select the secure check box as shown in Figure 27-14. Note that we have entered the IP address and port, not from the Telnet server, but from our Host On-Demand Redirector.



	Host Name or IP Address	LU or Pool Name	Port Number
Primary	9.24.105.39		12174
Backup 1			23
Backup 2			23

Connection Options

Connection Timeout 6 Seconds

☐ Auto-reconnect

☑ Try connecting to last configured host infinitely

Printer Association (only valid for TN3270E Display sessions)

Associated Printer Session

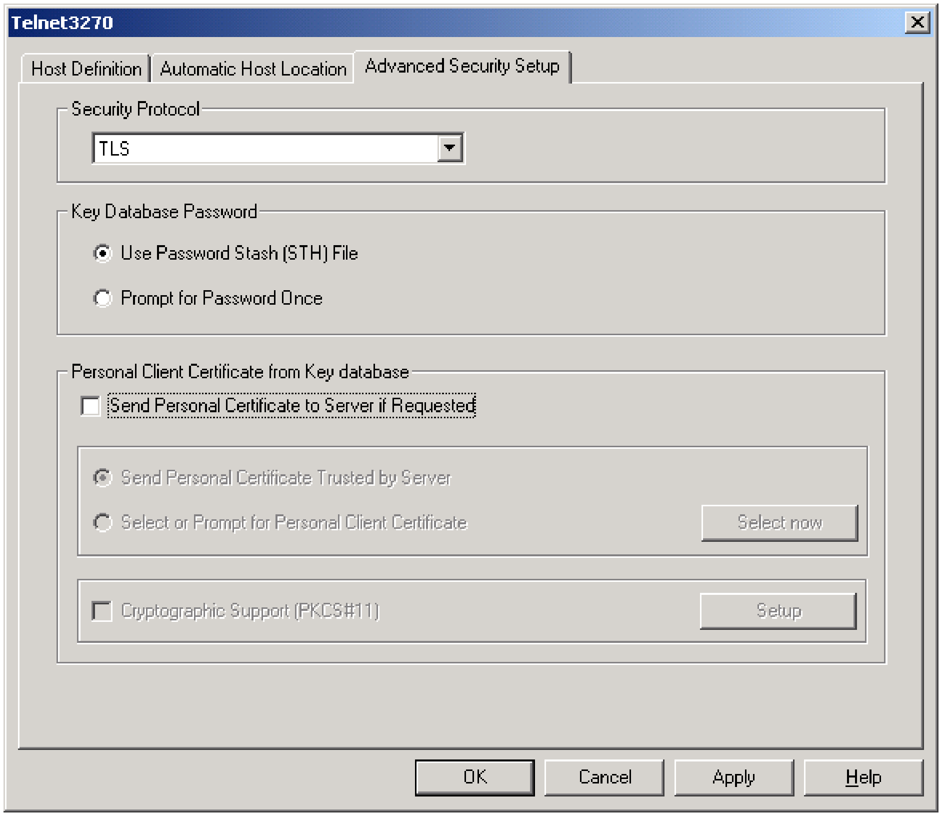
☑ Start Associated Printer Minimized

☑ Automatically close the associated printer session with this session

☑ Enable Security

Figure 27-14 Parameters for Telnet session

This is the only window in which we made entries. As reference we show in Figure 27-15 the tab Advanced Security Setup with its unchanged default values.


Telnet3270

Host Definition | Automatic Host Location | Advanced Security Setup

Security Protocol

TLS

Key Database Password

● Use Password Stash (STH) File

○ Prompt for Password Once

Personal Client Certificate from Key database

□ Send Personal Certificate to Server if Requested

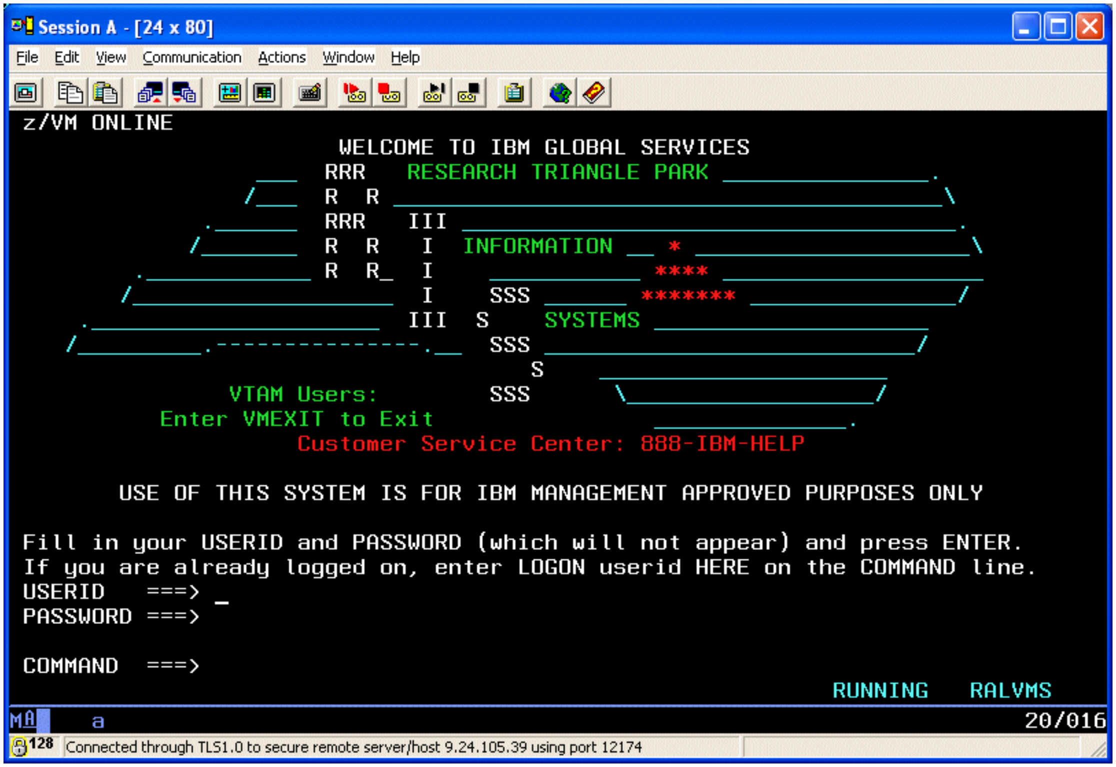
● Send Personal Certificate Trusted by Server

○ Select or Prompt for Personal Client Certificate

□ Cryptographic Support (PKCS#11)

Figure 27-15 Advanced tab of secure tn3270 session

Clicking **OK** through the panels back out produces the resulting TN3270 session from Personal Communications through our Host On-Demand Redirector to the mainframe in which the Telnet server runs.



```
z/VM ONLINE
                       WELCOME TO IBM GLOBAL SERVICES
                 ____ RRR   RESEARCH TRIANGLE PARK  _______________.
                /___  R  R _________________________________________\
             .______  RRR   III _____________________________________.
            /_______  R  R   I  INFORMATION __ * _____________________\
        .____________ R  R_  I    ___________ ****  ____________________
       /____________________ I    SSS ______ *******  ________________/
    ._______________________ III  S    SYSTEMS _____________________
   /_________.---------------.__  SSS  ____________________________/
                                      S   ______________________
               VTAM Users:        SSS     \___________________/
          Enter VMEXIT to Exit                    _______________.
                    Customer Service Center: 888-IBM-HELP

       USE OF THIS SYSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY

Fill in your USERID and PASSWORD (which will not appear) and press ENTER.
If you are already logged on, enter LOGON userid HERE on the COMMAND line.
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                           RUNNING   RALVMS
MA     a                                                             20/016
```

128 Connected through TLS1.0 to secure remote server/host 9.24.105.39 using port 12174

Figure 27-16 Secure TN3270 session with Personal Communications

In the status bar shown in Figure 27-16, we see the address and five digit port number of the Redirector. The TN server address is not known by the emulator and is not displayed. However, we see at the lower left corner a closed lock with a number. This shows us that we have a secure session with 128-bit encryption.

If your session fails to connect, did you stop and restart your Redirector after the certificate was created at the Host On-Demand?

27.2 Smart card support

A *smart card* is a small electronic device that contains electronic memory and may be used to store a single personal X.509 digital certificate. It does not hold the signer certificates. The signer certificate or the root and any intermediate certificate of the personal certificate on the smart card should be added in the PCommClientKeyDb.kdb file.

Some advantages of using a smart card are:

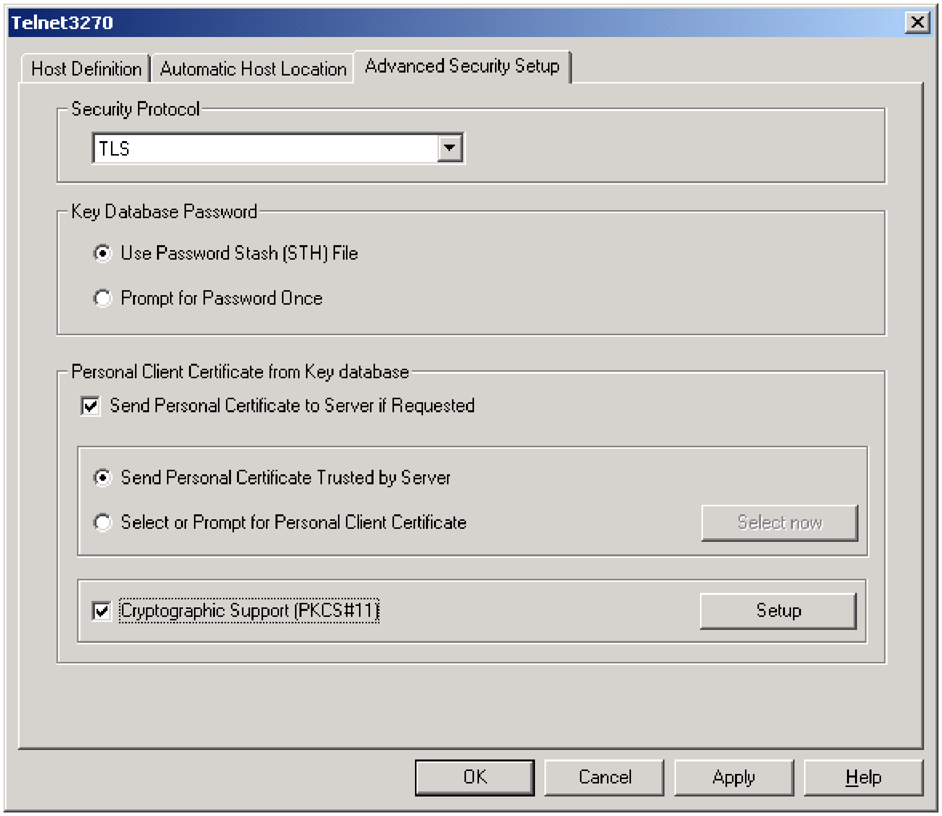
- Support for Netscape PKCS#11 cryptographic devices
- Allows you to store the Personal Certificates on the cryptographic devices. (for example, smart card, IBM embedded chips, and others)

- Provides additional security since the certificate is stored on an external physical device
- It takes two things to make a client-authenticated connection: something you have (the smart card) and something you know (the PIN password).
- This is considered safer than storing the certificate in the key database, PCommClientKeyDb.kdb file, on disk.

27.2.1 Enabling smart card support

To enable smart card support when configuring a session, perform the following steps:

1. Select **Enable Security** in the Host Definitions tab, then select the **Advanced Security Setup** tab. See Figure 27-17.



Security Protocol
TLS

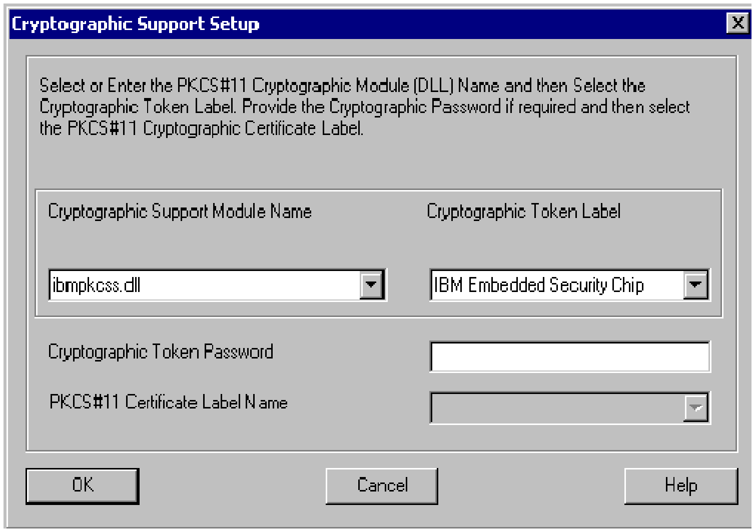
Key Database Password
● Use Password Stash (STH) File
○ Prompt for Password Once

Personal Client Certificate from Key database
☑ Send Personal Certificate to Server if Requested
● Send Personal Certificate Trusted by Server
○ Select or Prompt for Personal Client Certificate
☑ Cryptographic Support (PKCS#11)

Figure 27-17 Enable Security

2. On the Advance Security Setup tab, select **Send Personal Certificate to Server if Requested**.

3. To obtain the certificate from the smart card, select **Cryptographic Support (PKCS#11),** then click **Setup** to display the window shown in Figure 27-18.



Cryptographic Support Setup

Select or Enter the PKCS#11 Cryptographic Module (DLL) Name and then Select the Cryptographic Token Label. Provide the Cryptographic Password if required and then select the PKCS#11 Cryptographic Certificate Label.

Cryptographic Support Module Name: ibmpkcss.dll

Cryptographic Token Label: IBM Embedded Security Chip

Cryptographic Token Password:

PKCS#11 Certificate Label Name:

Figure 27-18 Smart card setup in Personal Communications

4. In the Cryptographic Support Setup window shown in Figure 27-18, choose the Netscape compatible PKCS#11 driver name from the drop-down list. If your provider’s driver is not found by Personal Communications, then you must manually enter a smart card driver name. Table 27-1 is a list of supported smart card drivers and their file names.

Table 27-1 Supported smart card drivers

Smart card Drivers	File names
IBM SecureWay Smartcard	w32pk2ig.dll
GemPlus/GemSoft Smartcard	w32pk2ig.dll
IBM Netfinity® PSG Chip[1]	ibmpkcss.dll
Rainbow Ikey 1000	Cryptoki22.dll
Schlumberger Cryptoflex	acpkcs.dll or slbck.dll
SCW PKCS 3GI 3-G International	3gp11csp.dll
Data Key	Dkck232.dll
Fortezza Module	fort32.dll

[1] The system boards in some IBM systems are preconfigured with a Promise of Value (POV) card, a 256-bit encrypted security chip daughtercard attached to the motherboard. If an attempt is made to remove the POV card from the board and install it into another system, the cryptographic key material will be erased, rendering it unusable. This security feature is by design and prevents the cryptographic key migration from one system to another. Therefore, moving this security chip from one board to another is not a supported option. If an attempt is made to move the POV card from one system to another, it may hang on boot and display an error message referring to an invalid machine type and serial number.

5. If the driver loaded successfully, the Cryptographic Token Label list is displayed. Now enter the Cryptographic Token Password (PIN). This provides access to the PKCS#11 cryptographic device and displays the PKCS#11 Certificate Label Name. If PKCS#11 cryptographic support is enabled and a password for the PKCS#11 cryptographic module is not defined during configuration, the user will be prompted to provide the password.

When you install support for a smart card, drivers are installed that allow you to store and retrieve your certificate from your smart card. Drivers are provided that allow both Netscape and Internet Explorer to access the certificate in the smart card. If your certificate was not pre-installed in the smart card for you by your administrator, you may use your browser to insert your certificate directly into the card.

If you have your certificate in a P12 file, you can use the certificate management utility to store the certificate on the PKCS#11 device if the ikmuser.properties file is updated with the right PKCS#11 module name.

Please refer to “Chapter 6” of the *Personal Communications Version 5.7 Administrator’s Guide and Reference,* SC31-8840 for further details.

27.3 Certificate Express Logon

In previous releases of Host On-Demand and z/OS, Certificate Express Logon was known as the Express Logon Feature (ELF). In Host On-Demand V8, the Express Logon feature was renamed to Certificate Express Logon.

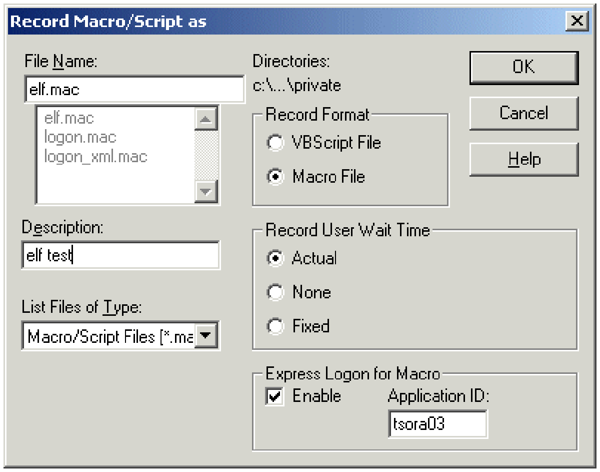
Personal Communications has been enhanced to support Certificate Express Logon. For a discussion of the concepts and operations of Certificate Express Logon, refer to 15.2, “Certificate Express Logon” on page 580. The remainder of this section will discuss the Personal Communication-specific implementations and operations regarding the Certificate Express Logon.

27.3.1 Client setup

The Certificate Express Logon requires an SSL session with client authentication; therefore, you first you must have Personal Communications configured for SSL and client authentication. Once the client-authenticated session is established, you may record the Certificate Express Logon macro.

Recording the Certificate Express Logon macro

From the menu bar of the emulator session, click **Actions -> Start Recording a Macro**. This results in the window shown in Figure 27-19.



File Name: elf.mac

Directories: c:\...\private

Record Format: ○ VBScript File ● Macro File

Description: elf test

List Files of Type: Macro/Script Files [*.ma

Record User Wait Time: ● Actual ○ None ○ Fixed

Express Logon for Macro: ☑ Enable Application ID: tsora03

Figure 27-19 Record Macro window for Certificate Express Logon

In this window you must select the radio button **Macro File,** since Certificate Express Logon macros can only be recorded in the native macro language of Personal Communications. Next, select **Enable** in the Express Logon for Macro field. In the Application ID field, fill in the Host Access Application ID that RACF uses to identify the desired application. This is *not* the VTAM APPLID of your host application. The Host Access Application ID is an ID that matches the RACF PTKTDATA profile configured at your OS/390 or z/OS host. Your RACF administrator will provide you with this ID, if they did not record and distribute the macro. Enter the name of the macro in the File Name field, and you may optionally provide a description of the macro in the Description field. Click **OK** to start the macro recording. In the OIA you will see the capital letter `R`, indicating that the recording process is taking place.

With the macro recording, return to the Personal Communications session and log on to your host application by typing in your host application name (`logon applid(application_name)`), your user ID, and your password. Note that in the logon statement the application_name entered *will be* the VTAM APPLID. The windows you see might vary, depending on your host systems. Enter your user ID and password when prompted.

Example 27-1 shows the results of the macro created for this chapter.

Example 27-1 Certificate Express Logon macro

```
Description =elf test
[wait sys]
"logon applid(ra03t)
[enter]
[wait inp inh]
wait 10 sec until FieldAttribute 0000 at (1,26)
wait 10 sec until cursor at (2,1)
[wait app]
elf applid tsora03
")USR.ID(
[enter]
[wait inp inh]
wait 10 sec until FieldAttribute 000C at (8,19)
wait 10 sec until cursor at (8,20)
[wait app]
")PSS.WD(
[enter]
```

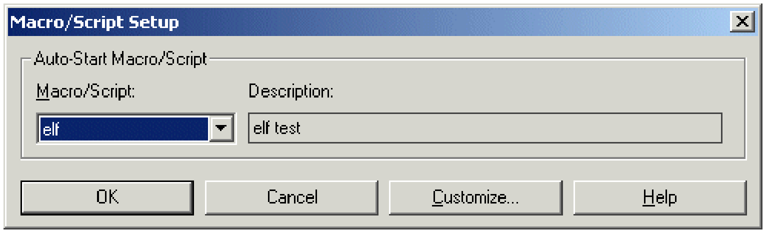
Notice the `elf` line after `[wait app]` and just prior to the user ID placeholder)`USR.ID(`. This line:

- Identifies the macro as being Certificate Express Logon enabled
- Saves the host access application ID entered on the record window in the application ID field

The real host user ID and password are replaced in the macro with special placeholder strings:

- The Certificate Express Logon user ID placeholder is)USR.ID(
- The Certificate Express Logon password placeholder is)PSS.WD(

To make the macro an autologon macro, click **Edit -> Preferences -> Macro/Script**, select your Certificate Express Logon macro from the Macro/Script drop-down list as shown in Figure 27-20, and click **OK**.



Macro/Script: elf

Description: elf test

Figure 27-20 Create an autologon macro

The next time you click that session in the Session Manager, it will open the session window, connect and run the Certificate Express Logon macro automatically.

28

Programming interfaces

Personal Communications has several programming interfaces that may be used to extend functionality, or more commonly to automate operations. The following application program interfaces (APIs) are available for use with Personal Communications Version 5.7:

- Protocol stack interfaces
  - SNA API - For details, see the online documentation *Client/Server Communications Programming* (pccsp.pdf), SC31-8479.
- Emulator interfaces
  - Macros
  - EHLLAPI - For details, see the online documentation *Emulator Programming*, (pcep.pdf).
  - HACL - For details, see the online documentation *Client/Server Communications Programming* (pccsp.pdf), SC31-8479, “Part 5” and the online documentation *Host Access Class Library* (pcecl.pdf), SC31-8685, and the online documentation in the CD subdirectory \publications\en_US\doc\hacl\.
  - OLE

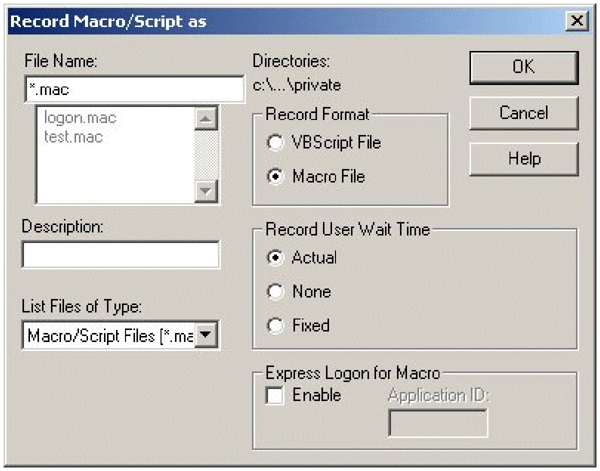
28.1 Macros

This section focuses only on the following:

- Converting macro to XML
- Importing macros into Host On-Demand
- Hiding logon passwords

28.1.1 Converting macro to XML

Personal Communications records keyboard macros either in its native language or in VBSCRIPT. However, the Convert Macro utility will not convert VBSCRIPT macros; it will only convert macros recorded and stored in the native Personal Communications language (Record Format = Macro File).



Record Macro/Script as

File Name: *.mac

logon.mac
test.mac

Directories: c:\...\private

Record Format
○ VBScript File
● Macro File

Description:

List Files of Type: Macro/Script Files [*.ma

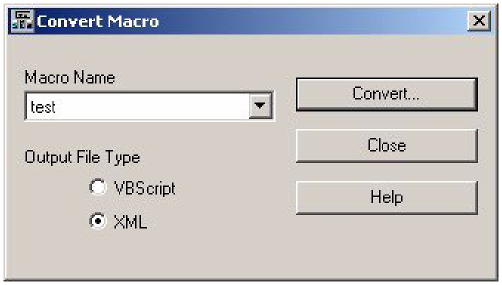
Record User Wait Time
● Actual
○ None
○ Fixed

Express Logon for Macro
□ Enable
Application ID:

Figure 28-1 Recording a macro as a native macro file

Personal Communications provides a utility that is intended for use by customers who are migrating from Personal Communications to Host On-Demand. This utility will convert Personal Communications macros into an XML format that may be imported into Host On-Demand. Note that there is no utility available to migrate from XML or VBscript to the Personal Communications macro file format.

To convert a macro to XML, click **Start -> Programs -> IBM Personal Communications -> Utilities -> Convert Macro**.



Macro Name
test

Output File Type
○ VBScript
● XML

Figure 28-2 Convert Macro utility

If you cannot find your recorded macro, it is possible that you did not record it in the native macro file.

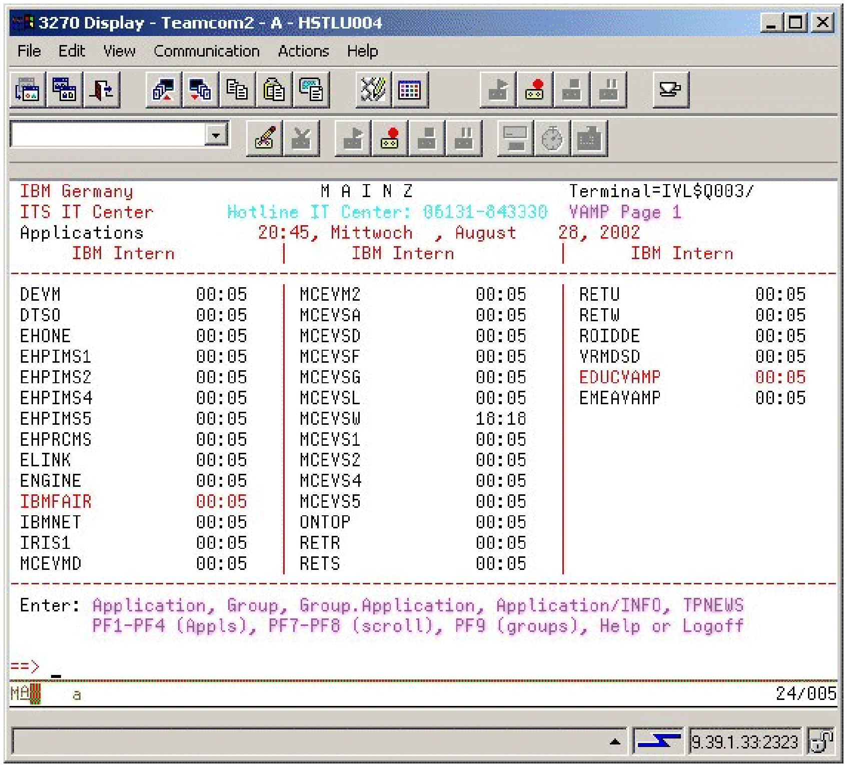
> **Important:** Always check output for comments (unconverted statements). See the example in 28.1.3, “Hiding logon passwords” on page 988.

Refer to Personal Communications documentation for more information on the enhanced macro conversion utility introduced in Personal Communications V5.6. The Convert Macro utility converts recorded native Personal Communications macros into XML or VMScript. The macro must exist in the application data directory specified during installation of Personal Communications. The macro conversion utility has been enhanced to allow saving the converted file into a location that you specify.

28.1.2 Importing macros into Host On-Demand

A macro converted to XML using the Convert Macro utility can be imported into Host On-Demand as shown in the following example. It is not required to change the extension from .mac to .xml to import the macro to Host On-Demand.

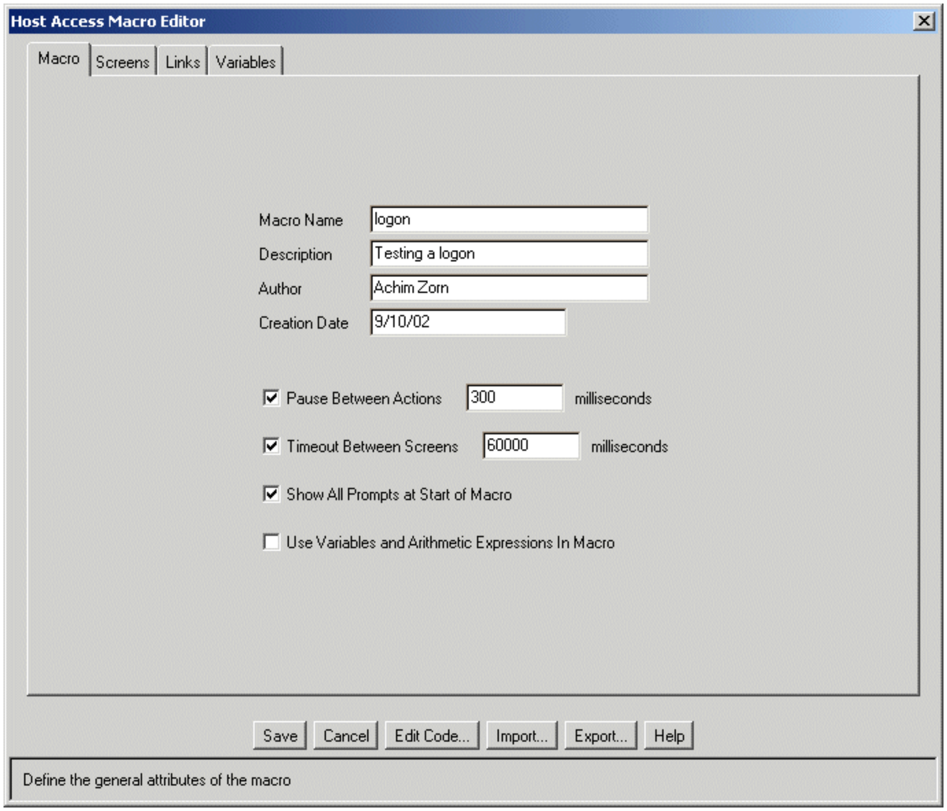
To import the macro into Host On-Demand, you must enable your Host On-Demand session so that you show the toolbar with the Macro Manager portion enabled as shown in Figure 28-3. This may be done by clicking **View -> Macro Manager** from the menu bar.



```
IBM Germany                  M A I N Z          Terminal=IVL$Q003/
ITS IT Center       Hotline IT Center: 06131-843330  VAMP Page 1
Applications           20:45, Mittwoch  , August    28, 2002
     IBM Intern             |      IBM Intern          |      IBM Intern
---------------------------------------------------------------------------------
DEVM             00:05 | MCEVM2           00:05 | RETU             00:05
DTSO             00:05 | MCEVSA           00:05 | RETW             00:05
EHONE            00:05 | MCEVSD           00:05 | ROIDDE           00:05
EHPIMS1          00:05 | MCEVSF           00:05 | VRMDSD           00:05
EHPIMS2          00:05 | MCEVSG           00:05 | EDUCVAMP         00:05
EHPIMS4          00:05 | MCEVSL           00:05 | EMEAVAMP         00:05
EHPIMS5          00:05 | MCEVSW           18:18 |
EHPRCMS          00:05 | MCEVS1           00:05 |
ELINK            00:05 | MCEVS2           00:05 |
ENGINE           00:05 | MCEVS4           00:05 |
IBMFAIR          00:05 | MCEVS5           00:05 |
IBMNET           00:05 | ONTOP            00:05 |
IRIS1            00:05 | RETR             00:05 |
MCEVMD           00:05 | RETS             00:05 |
---------------------------------------------------------------------------------
Enter: Application, Group, Group.Application, Application/INFO, TPNEWS
       PF1-PF4 (Appls), PF7-PF8 (scroll), PF9 (groups), Help or Logoff

==> _
MA     a                                                               24/005
```

Figure 28-3 Host On-Demand session with toolbar for managing macros

Next, click the edit icon from the Macro Manager toolbar to open the window for importing the XML macro from Personal Communications, as shown in Figure 28-4.



Macro Name: logon
Description: Testing a logon
Author: Achim Zorn
Creation Date: 9/10/02

☑ Pause Between Actions 300 milliseconds
☑ Timeout Between Screens 60000 milliseconds
☑ Show All Prompts at Start of Macro
☐ Use Variables and Arithmetic Expressions In Macro

Define the general attributes of the macro

Figure 28-4 Fill in the fields and use Import

Click **Import** to display the window in which you may select the files available for import. Navigate if necessary to the location containing the macro and select it. When the macro is read, the fields in the window are completed using the information contained in the headers of the imported macro. You can update the fields manually by overtyping.

After the file is imported, you can change the macro if desired, then click **Save** to store the macro with the session properties.

Certificate Express Logon macros can also be imported from Personal Communications to Host On-Demand and used by Host On-Demand.

The user should look at the converted file to make sure all functions were converted correctly. If there is an unsupported macro function, it is put into the output file as an `xml comment` line.

28.1.3 Hiding logon passwords

One of the most popular macros is a logon macro. By default, macro recording will capture and store passwords in the clear even though they are not displayed on the host screen. The contents of the host screen contain the password, but the display attribute of that field is hidden so that the data cannot be seen. Administrators can modify the client workstation profile (*.WS) in the `[keyboard]` stanza with the following option:

```
   HideNonDisplayDataOnRecord=Y
```

With this in the *.ws file, the macro recording process will place `[input nd]` into the macro instead of the actual password, as shown in Example 28-1. When the macro is replayed in Personal Communications, a Windows prompt for the user's password will be issued, and the password will not be displayed while typing.

Example 28-1 Workstation profile

```
[Profile]
ID=WS
Version=6

[Telnet3270]
HostName=9.39.1.11
Security=N
AutoReconnect=Y
HostPortNumber=23

[Communication]
Link=telnet3270
[3270]
QueryReplyMode=Auto
HostCodePage=037-U

[Keyboard]
HideNonDisplayDataOnRecord=Y
CuaKeyboard=1
Language=United-States
DefaultKeyboard=$$BLANK$$
Example for the resulting native macro as recorded:
Description =
[wait app]
"devm zorn
[enter]
[wait inp inh]
```

```
wait 10 sec until FieldAttribute 000C at (22,80)
wait 10 sec until cursor at (23,1)
[wait app]
[input nd]
[enter]
```

A translation of that macro into VBSCRIPT will also contain the equivalent command for `[input nd]`.

When converting this macro into XML for Host On-Demand, the `[input nd]` line is not recognized; therefore, it will be commented within the XML macro during translation:

```
/<comment> ********* The following line is not translatable to HOD/XML---
[input nd]
```

In such cases where there is no equivalent for a Personal Communications macro command in XML, you must build your own workaround with the available set of XML commands. Available XML macro commands and their descriptions are located in the Host Access Toolkit online documentation *Host Access Beans for Java Reference*. Specifically, for entering a password, the following command should be inserted at the point where the password should be entered:

```
<prompt name="password" description="" row="29" col="17" len="8" default=""
clearfield="true" encrypted="true" movecursor="false" xlatehostkeys="false"
/>
```

where the following definitions apply:

`row` The row to place the prompt. The value must be a number. This is a required element.

`col` The column to place the prompt. The value must be a number. This is a required element.

`len` The length of the prompt. The value must be a number. This is a required element.

`name` The name of the prompt. This can be any valid unicode character. This element is optional.

`description` The description of the prompt. This can be any valid unicode character. This element is optional.

`default` The prompt's default value. This can be any valid unicode character. This element is optional.

`clearfield` This clears the host field on placement of prompt text. The value must be `true` or `false`. This element is optional. The default is `false`.

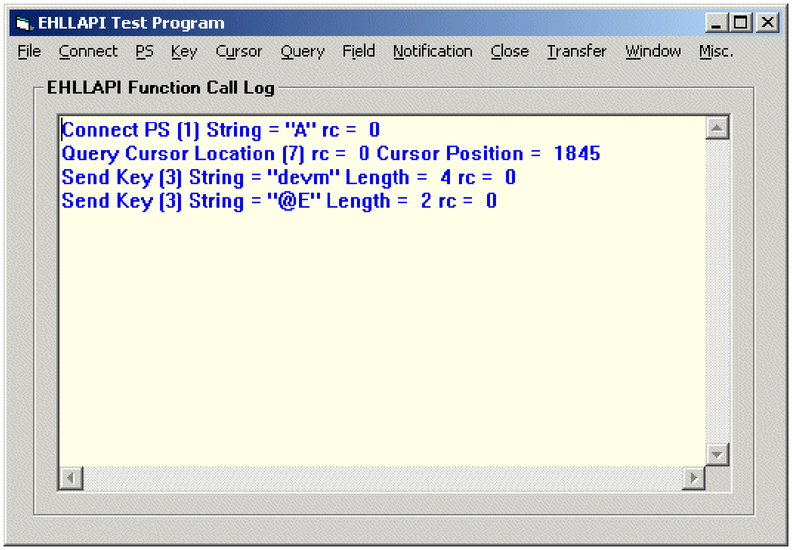
`encrypted` This element is optional, and must be either `true` or `false`. If the value is `true` then a password echo character will be displayed (*) as the password is typed. The default is `false`.

`xlatehostkeys` If `true`, host key mnemonics (for example, `[enter]`) will be translated. For a list of key mnemonics, see “Appendix A, SendKeys Mnemonic Keywords” in the *Host Access Class Library,* SC31-8685 document. The value must be `true` or `false`. This attribute is optional. The default is `false`. If you do not have this value set to `true`, which is normal because you wouldn't ask users to type key mnemonics, don't forget to code an input element after the prompt(s) for the current actions to get the prompt data entered onto the host.

28.2 EHLLAPI

High Level Application Program Interface (HLLAPI) and Enhanced HLLAPI (EHLLAPI) are standard program interfaces to many emulator types. They are simple to use and can be used by various programming languages. There are no new functions in Personal Communications Version 5.7, but we wanted to add some hints in this book because all other interfaces to the presentation space are bridged through EHLLAPI.

Personal Communication provides a tool (vbhllapi.exe) for testing single EHLLAPI commands. It is located at the CD of the product in the subdirectory \install\pcomm\program files\Ibm\Personal\Communications\samples\vbhllapi.



EHLLAPI Test Program
File Connect PS Key Cursor Query Field Notification Close Transfer Window Misc.
EHLLAPI Function Call Log

```
Connect PS (1) String = "A" rc =  0
Query Cursor Location (7) rc =  0 Cursor Position =  1845
Send Key (3) String = "devm" Length =  4 rc =  0
Send Key (3) String = "@E" Length =  2 rc =  0
```

Figure 28-5 EHLLAPI test program

The following sequence was tested with the EHLLAPI test tool and recorded in Figure 28-5. For details on EHLLAPI commands and their return codes, refer to Chapter 3 of the online documentation *Emulator Programming,* pcep.pdf.

The sequence connects to the presentation space of display session A, queries the cursor position, and sends a string and the Enter key to that session.

1. Start a display session A. Now use the EHLLAPI test tool as follows.
2. Click **Connect** and **Connect PS.**

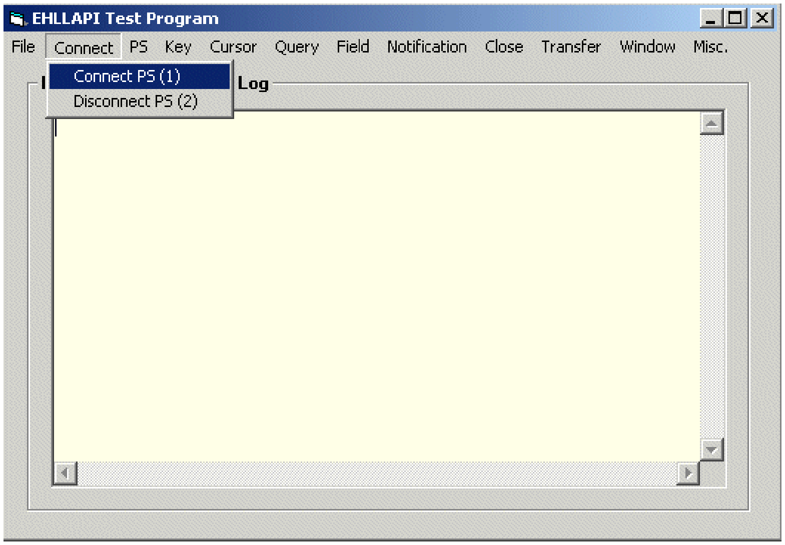
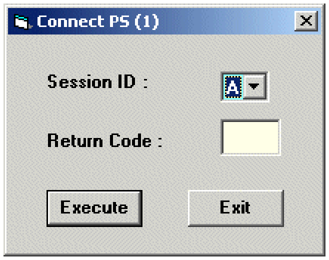


Figure 28-6 Starting EHLLAPI test tool and connecting a presentation space

3. Enter the short session ID to which you want to connect and then click **Execute**. Note that the number in parentheses after the command is the command number as referred to in the online documentation *Emulator Programming*. After the command is executed, it returns a return code, which is zero for a successful completion. After that, click **Exit** to leave the window.



Session ID : A

Return Code :

Figure 28-7 Connect Presentation Space (PS) window

4. In the HLLAPI test program panel, click **Cursor** and select **Query**.
5. Click **Execute** and then **Exit**.

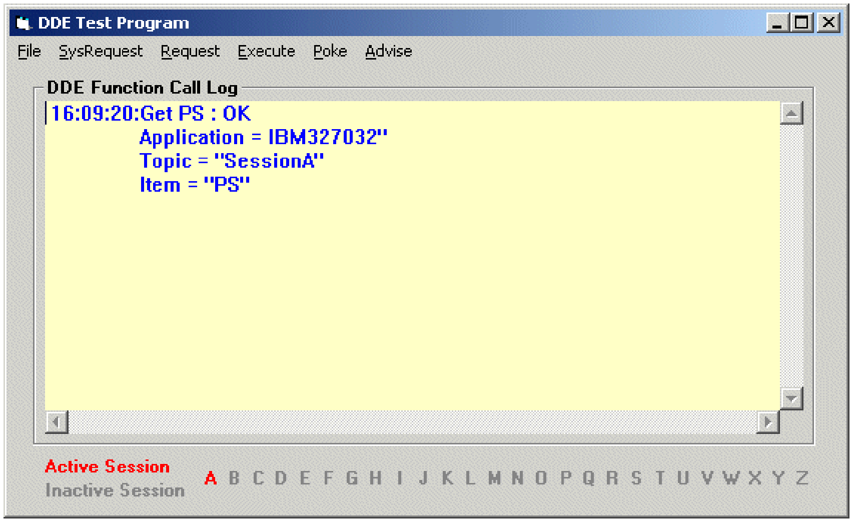
Note that the window in the EHLLAPI test program is filled with the commands, the corresponding parameters, and return values and return codes.

According to the previous commands, we subsequently used **Key -> Send Key** once for sending the string `devm` to the presentation space, and afterwards used the same command to send the Enter key.

The Personal Communications session window shows the appropriate responses, just as if someone has typed in `devm` and pressed the Enter key.

All actions that have been recorded in the EHLLAPI Test Program can be saved by clicking **File -> Save Log As...** from the menu bar.

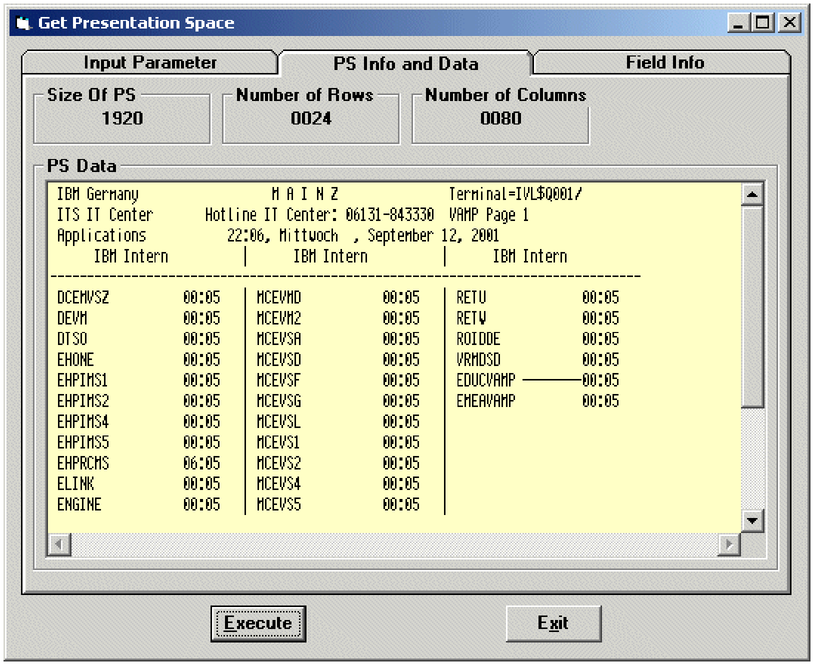
The equivalent test tool (vbdde.exe) is available for Dynamic Data Exchange (DDE) in the subdirectory \install\program files\Ibm\Personal Communications\samples\vbdde.



```
16:09:20:Get PS : OK
          Application = IBM327032"
          Topic = "SessionA"
          Item = "PS"
```

Figure 28-8 DDE Test Program

Figure 28-8 shows the content of the DDE test program after clicking **Request -> Get PS** and selecting session **A.**



Size Of PS: 1920

Number of Rows: 0024

Number of Columns: 0080

PS Data

```
IBM Germany                  M A I N Z              Terminal=IVL$Q001/
ITS IT Center       Hotline IT Center: 06131-843330 VAMP Page 1
Applications           22:06, Mittwoch  , September 12, 2001
     IBM Intern            |      IBM Intern            |      IBM Intern
-------------------------------------------------------------------------------
DCEMVSZ          00:05     | MCEVMD           00:05     | RETU             00:05
DEVM             00:05     | MCEVM2           00:05     | RETV             00:05
DTSO             00:05     | MCEVSA           00:05     | ROIDDE           00:05
EHONE            00:05     | MCEVSD           00:05     | VRMDSD           00:05
EHPIMS1          00:05     | MCEVSF           00:05     | EDUCVAMP         00:05
EHPIMS2          00:05     | MCEVSG           00:05     | EMEAVAMP         00:05
EHPIMS4          00:05     | MCEVSL           00:05     |
EHPIMS5          00:05     | MCEVS1           00:05     |
EHPRCMS          06:05     | MCEVS2           00:05     |
ELINK            00:05     | MCEVS4           00:05     |
ENGINE           00:05     | MCEVS5           00:05     |
```

Figure 28-9 Request Get PS with DDE Test Tool

28.3 HACL

In Personal Communications Version 5.7, no new Host Access Class Library (HACL) functions have been added. For details on how to write applications that utilize HACL, please refer to the online documentation *Host Access Class Library,* SC31-8685 (pcecl.pdf), and “Chapter 9” in the redbook *Personal Communications Version 4.3 for Windows 95, 98 and NT,* SG24-4689.

29

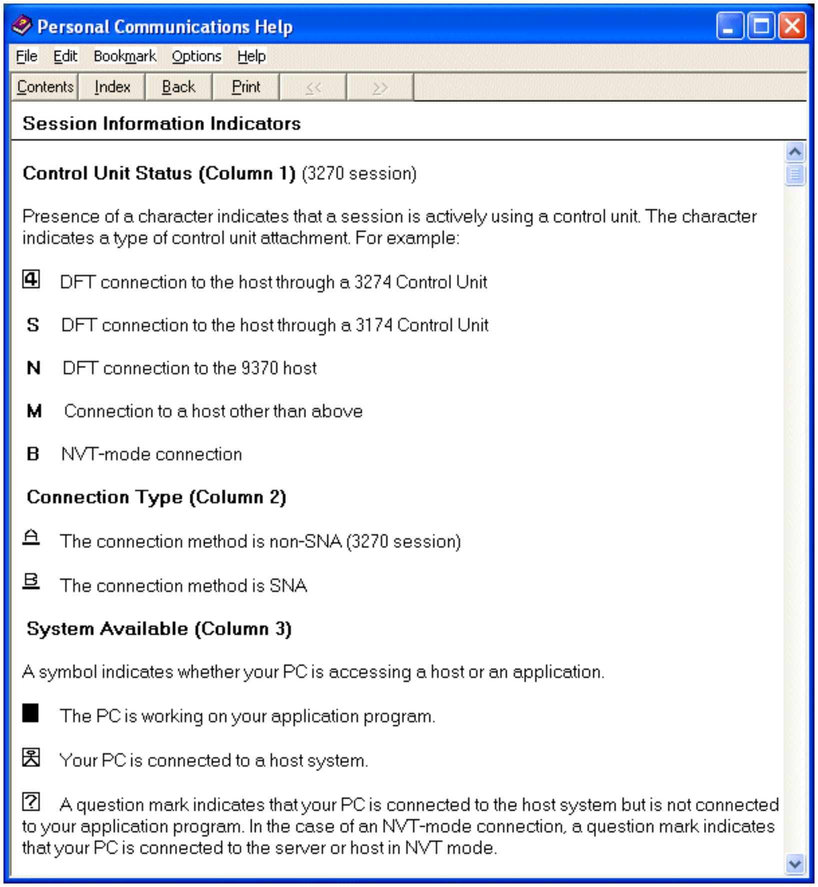
Problem determination

When you experience a problem, a number of methods and tools are available to find the cause. In many cases, problems occur due to configuration errors somewhere at and between the endpoints. This chapter covers some of the most important tools in Personal Communications to help resolve problems.

29.1 Operator information area (OIA)

The operator information area is the text row below the blue separator line at the bottom of the Personal Communications window. This OIA is common to most hardware terminal types and emulators. Its content is controlled by the host and controllers.

The left part of the OIA shows general information about the current state of the connection and host type, and the right part of the OIA shows the current cursor position in the line/column format. For details and an explanation of the messages from the emulator menu bar, click **Help -> Help Contents -> The Operator information area messages** to display the OIA help window shown in Figure 29-1.


Personal Communications Help
File Edit Bookmark Options Help
Contents Index Back Print << >>

Session Information Indicators

Control Unit Status (Column 1) (3270 session)

Presence of a character indicates that a session is actively using a control unit. The character indicates a type of control unit attachment. For example:

4 DFT connection to the host through a 3274 Control Unit

S DFT connection to the host through a 3174 Control Unit

N DFT connection to the 9370 host

M Connection to a host other than above

B NVT-mode connection

Connection Type (Column 2)

A The connection method is non-SNA (3270 session)

B The connection method is SNA

System Available (Column 3)

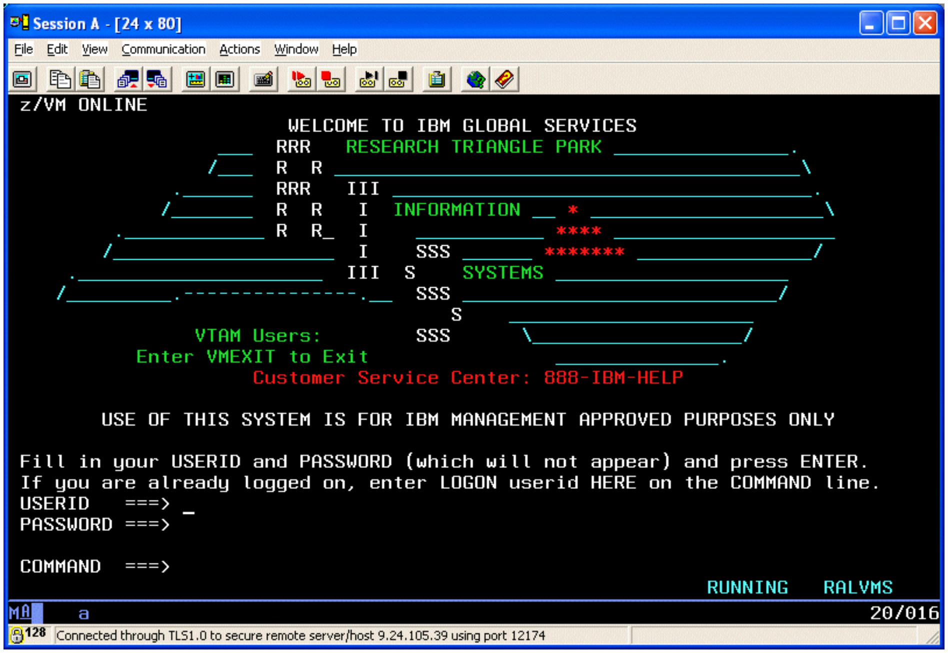
A symbol indicates whether your PC is accessing a host or an application.

■ The PC is working on your application program.

⊠ Your PC is connected to a host system.

? A question mark indicates that your PC is connected to the host system but is not connected to your application program. In the case of an NVT-mode connection, a question mark indicates that your PC is connected to the server or host in NVT mode.

Figure 29-1 Help window for OIA on a 3270 session



```
z/VM ONLINE
                       WELCOME TO IBM GLOBAL SERVICES
                 ___  RRR   RESEARCH TRIANGLE PARK _______________.
                /___  R   R _________________________________________\
             .______  RRR   III  ___________________________________.
            /_______  R   R  I   INFORMATION __ * ___________________\
        .____________ R   R_ I    ___________ **** ___________________
       /___________________  I    SSS ______ ******* _______________/
    ._____________________  III  S    SYSTEMS ____________________
   /_________.---------------.__  SSS ___________________________/
                                     S    _____________________
               VTAM Users:        SSS      \___________________/
          Enter VMEXIT to Exit                ______________.
                    Customer Service Center: 888-IBM-HELP

       USE OF THIS SYSTEM IS FOR IBM MANAGEMENT APPROVED PURPOSES ONLY

Fill in your USERID and PASSWORD (which will not appear) and press ENTER.
If you are already logged on, enter LOGON userid HERE on the COMMAND line.
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                           RUNNING   RALVMS
MA    a                                                               20/016
```

128 Connected through TLS1.0 to secure remote server/host 9.24.105.39 using port 12174

Figure 29-2 TN3270 session using 128-bit encryption

Using Figure 29-2, we interpret the OIA:

- The M in position 1 means that the host connection is not a DFT or Network Virtual Terminal NVT connection.
- The A indicates a non-SNA connection.
- The stick-man in the box indicates that you are connected to the host VTAM system. When the stick-man turns into a solid box, you will be connected to your application.
- The 20/016 at the far right of the OIA states that the cursor is at row 20, column 16.

In case of a problem during a printer or display session, the status of the OIA will provide important information. For detailed information, use the Help option from the menu bar. For an explanation of error codes, click **Help -> Contents -> When you encounter a Problem** from the menu bar.

For help with error messages that are not displayed in the OIA, but that pop up in an error message window, click **Help -> Help Contents -> Contents** from the menu bar, and then use the tabulator **Find**.

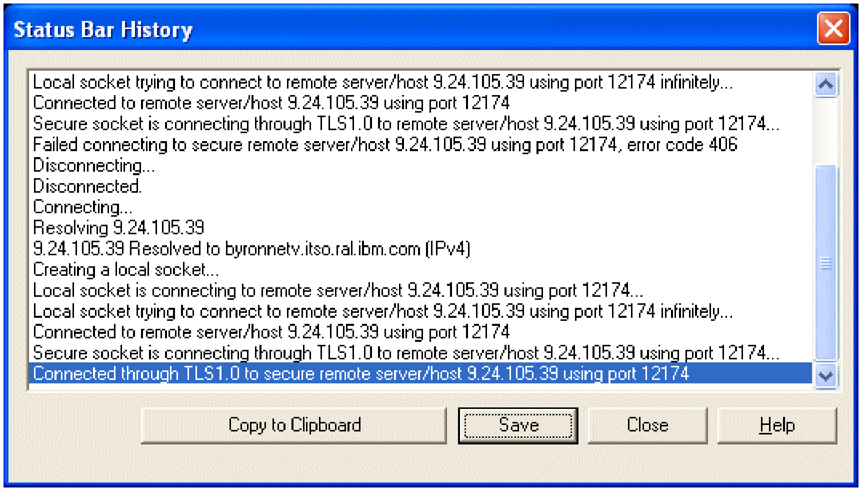
29.2 Status bar

The grey field below the OIA is the status bar (see Figure 29-2). It contains additional details about the session status, and its content is generated by Personal Communications.

The left-most section indicates the security status:

- A non-secure session is indicated with an open padlock.
- A secure session is indicated with a locked padlock and the level of encryption will be indicated with a number. In Figure 29-2, the session is shown secure using 128-bit TLS encryption.

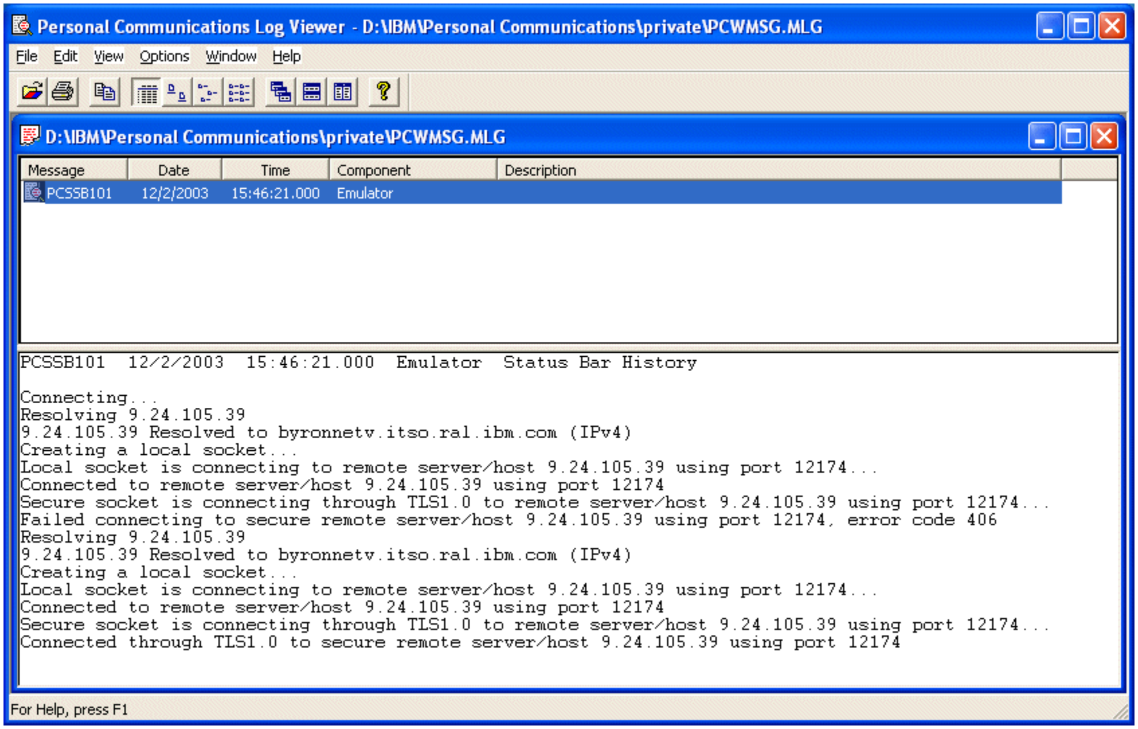
The next section of the status bar is used to contain the current status of the connection. A history of the messages that appear here may be viewed by clicking (from the menu bar) **View -> Status Bar History.** A window like the one shown in Figure 29-3 will appear.



```
Local socket trying to connect to remote server/host 9.24.105.39 using port 12174 infinitely...
Connected to remote server/host 9.24.105.39 using port 12174
Secure socket is connecting through TLS1.0 to remote server/host 9.24.105.39 using port 12174...
Failed connecting to secure remote server/host 9.24.105.39 using port 12174, error code 406
Disconnecting...
Disconnected.
Connecting...
Resolving 9.24.105.39
9.24.105.39 Resolved to byronnetv.itso.ral.ibm.com (IPv4)
Creating a local socket...
Local socket is connecting to remote server/host 9.24.105.39 using port 12174...
Local socket trying to connect to remote server/host 9.24.105.39 using port 12174 infinitely...
Connected to remote server/host 9.24.105.39 using port 12174
Secure socket is connecting through TLS1.0 to remote server/host 9.24.105.39 using port 12174...
Connected through TLS1.0 to secure remote server/host 9.24.105.39 using port 12174
```

Figure 29-3 Status Bar History window

Telnet sessions do not automatically place entries into the PCWMSG.MLG file; however, from this window, you may save the contents of the history window into the PCWMSG.MLG file, where you can then use the Log Viewer (see Figure 29-4) to examine the entries.


Personal Communications Log Viewer - D:\IBM\Personal Communications\private\PCWMSG.MLG
File Edit View Options Window Help
D:\IBM\Personal Communications\private\PCWMSG.MLG

Message	Date	Time	Component	Description
PCSSB101	12/2/2003	15:46:21.000	Emulator	

```
PCSSB101  12/2/2003  15:46:21.000  Emulator  Status Bar History

Connecting...
Resolving 9.24.105.39
9.24.105.39 Resolved to byronnetv.itso.ral.ibm.com (IPv4)
Creating a local socket...
Local socket is connecting to remote server/host 9.24.105.39 using port 12174...
Connected to remote server/host 9.24.105.39 using port 12174
Secure socket is connecting through TLS1.0 to remote server/host 9.24.105.39 using port 12174...
Failed connecting to secure remote server/host 9.24.105.39 using port 12174, error code 406
Resolving 9.24.105.39
9.24.105.39 Resolved to byronnetv.itso.ral.ibm.com (IPv4)
Creating a local socket...
Local socket is connecting to remote server/host 9.24.105.39 using port 12174...
Connected to remote server/host 9.24.105.39 using port 12174
Secure socket is connecting through TLS1.0 to remote server/host 9.24.105.39 using port 12174...
Connected through TLS1.0 to secure remote server/host 9.24.105.39 using port 12174
```

Figure 29-4 Log Viewer displaying Status Bar History saved data

> **Note:** The Status Bar History entries are not logged separately in the PCSWMSG.MLG file. The are merged into the existing PCWMSG.MLG with the remark `Emulator` in the Component column (see Figure 29-4).

29.3 Tracing/bundling problem determination data

The Trace Facility is able to monitor and record a number of parameters. It can be started in one of the following ways:

- Through the Windows Start menu. Click **Start -> Programs -> IBM Personal Communications -> Administrative and PD Aids -> Trace Facility**.
- Through the menu bar of a Personal Communications Session. Click **Actions -> Launch -> Trace Facility**.

- Through the command line, issue the command `cstrace`.

Before a trace is started, the session and the node (if SNA is used) should be stopped first so that the start of the link and of the session will be captured in the trace. Then follow these steps:

1. Start the trace.
2. Start the session.
3. Recreate the problem.
4. At the point where the problem occurs, take a copy of the window or screen by one of the following methods:
   - Alt+Print Screen for the active window
   - Ctl+Print Screen for the complete screen content
5. Stop the trace.
6. Record the steps that were taken to recreate the problem. Use WordPad to record the steps.
7. Paste the content of the clipboard, which contains the screen copy of the problem, into the readme file.
8. Store the readme file in your Application Data Location along with your configuration files so that it will be saved by the Information Bundler.
9. After the trace has been taken, save and format it in your Application Data Location.
10. Use the Information Bundler to collect the trace and relevant data for Personal Communications Version 5.7 from your Application Data Location:
    a. Start the Information Bundler from the menu bar of a session by clicking **Actions -> Launch -> Information Bundler,** or by clicking **Start -> Programs -> IBM Personal Communications -> Administrative and PD Aids -> Information Bundler.**

    b. A self-extracting file named x12345.exe will be created and placed in the subdirectory where all configuration files of Personal Communications Version 5.7 reside (which depends on options set during installation).
11. Send the information to IBM support.

29.4 Tracing from the command line

CSTRACE command options

In some cases, it is helpful to start the trace through the command line. Examples ar as follows:

- When only a command prompt is available, such as when doing a remote control of a workstation
- If it is easier to send a batch file with the trace commands to users instead of guiding them through the graphical interface.

Tracing execution and formatting are performed using the **cstrace** command. The options and syntax are listed here:

- `APPLY [-f function_ID -c component_ID -o trace_options] [-r] [-t trunc_length]`

  This command affects dynamic changes to the currently running options, where:

`-f function_id`	Specifies the function (group) to trace, where `function_id` is an integer. If you specify the `-f` flag, you must also specify the `-c` and `-o` flags.
`-c component_ID`	Specifies the component to trace, where `component_id` is an integer
`-o trace_options`	Specifies the trace options to use, where `trace_options` is a hex value, where the value has leading zeros, those zeros are optional.
`-r`	Clears the trace buffer.
`-t trunc_length`	Specifies the maximum trace data length, where `trunc_length` is an integer between 992 and 131072. The default is 16352.

- `FORMAT[filename]`

  This command converts the trace data to a human-readable log. The default file is nstrc.trc. If you specify `[filename]`, the file must specify the extension `.trc`.

- `RESET`

  Use this command when you wish to discard the current trace data.

- `SAVE [-a] [filename]`

  Issue this command to save the current trace data to a file. If you specify the `-a` flag, the data is appended to the file. The default is to overwrite the current trace data. `[filename]` is the name of the file to save.

- `SHUTDOWN`

  This shuts down the trace facility, and exits the program.

- `START [-f function_ID -c component_ID -o trace_options] [-r] [-t trunc_length] [-s]`

Use this command to start the trace facility. You may optionally specify the following options at startup, or later use the APPLY option to change them.

`-f function_id` Specifies the function (group) to trace, where `function_id` is an integer. If you specify the `-f` flag, you must also specify the `-c` and `-o` flags.

`-c component_ID` Specifies the component to trace, where `component_id` is an integer

`-o trace_options` Specifies the trace options to use, where `trace_options` is a hex value, where the value has leading zeros; those zeros are optional.

`-r` Reset the trace buffer.

`-t trunc_length` Specifies the maximum trace data length, where `trunc_length` is an integer between 992 and 131072. The default is 16352.

`-s storage_number` Specifies the number of blocks in the trace buffer

`-b block size` Specifies the size of a block in the trace buffer

`-l list file` Specifies a file containing a list with the required trace options in a .dat file

- `STATUS`

  Displays the current active trace and all its options.

- `STOP [-f function_ID -c component_ID -o trace_options]`

  Suspends one or more active trace options. If you do not specify an option, all active traces are suspended:

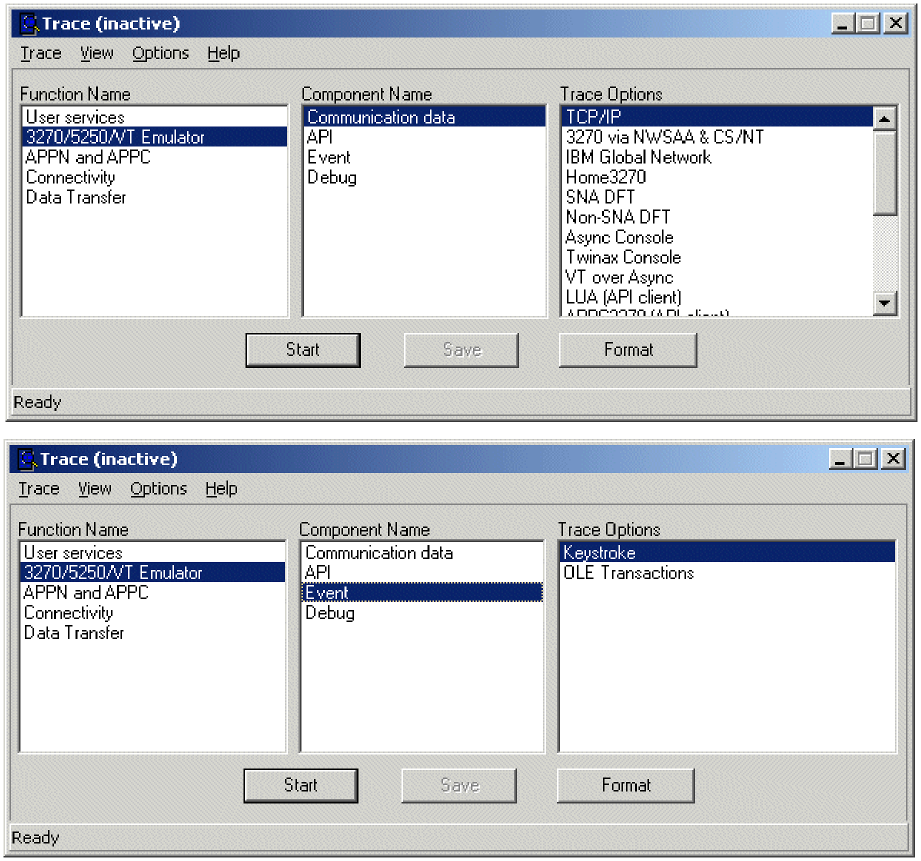
`-f function_id` Specifies the function (group) to trace, where `function_id` is an integer. If you specify the `-f` flag, you must also specify the `-c` and `-o` flags.

`-c component_ID` Specifies the component to trace, where `component_id` is an integer

Note: Please look up the parameter values for the functions, components, and options in the file nstrc.cfg located in the subdirectory \en_US\ of your installation path of Personal Communications Version 5.7. Use only a text browser to view that file. Changes to that file will cause the trace function to produce unexpected results.

29.4.1 Example TCP/IP trace from command line

When traces are taken using the graphical interface, users must select the options as shown in Figure 29-5.



Function Name
User services
3270/5250/VT Emulator
APPN and APPC
Connectivity
Data Transfer

Component Name
Communication data
API
Event
Debug

Trace Options
TCP/IP
3270 via NWSAA & CS/NT
IBM Global Network
Home3270
SNA DFT
Non-SNA DFT
Async Console
Twinax Console
VT over Async
LUA (API client)

Function Name
User services
3270/5250/VT Emulator
APPN and APPC
Connectivity
Data Transfer

Component Name
Communication data
API
Event
Debug

Trace Options
Keystroke
OLE Transactions

Figure 29-5 Graphical trace selections

You can issue the following commands in a batch file to set the same trace parameters as shown in Figure 29-5:

```
cstrace stop
cstrace start
cstrace apply /f 2 /c 1 /o 1
cstrace apply /f 2 /c 3 /o 10000
cstrace status
```

You have to apply the different trace functions in separate **apply cstrace** commands. The response on the screen to the cstrace status is as follows.

```
C:\>cstrace status
Current Active Trace:

GROUP: 3270/5250/VT Emulator  (2)
COMPONENT: Communication data  (1)
FLAG: TCP/IP  (1)

GROUP: 3270/5250/VT Emulator  (2)
COMPONENT: Event  (3)
FLAG: Keystroke  (10000)
```

To stop and save the trace, we used the following sequence in a second batch file:

```
cstrace stop
cstrace save nstrc.trc
cstrace format nstrc.trc
copy *.nstrc "c:\program files\ibm\personal communications\private"
cd "c:\program files\ibm\personal communications\private"
dir nstrc*.*
```

The screen response is as follows:

```
Volume in drive C has no label.
 Volume Serial Number is F48E-B3E4

 Directory of c:\Program Files\IBM\Personal Communications\private

08/28/2002  03:46p               6,296 nstrc.tlg
08/28/2002  03:46p               2,038 nstrc.trc
08/28/2002  03:46p                   0 nstrcips.trc
               3 File(s)          8,334 bytes
               0 Dir(s)  14,090,272,768 bytes free
```

In this example, we copied the resulting trace files to the subdirectory where we keep our configuration files for Personal Communications. From there, all data will be copied when the information bundler is used to collect data for problem determination.

Instead of typing all trace options into the command line or using a batch file, you can use a trace option file. For usage and contents of the trace option file, refer to “CSTRACE command options” on page 1000. A command using a trace option file would be as follows:

```
cstrace start /l c:\pcomm_path\nstrc.dat
```

A sample file, NSTRC.DAT, containing all possible trace settings is supplied with the CD of Personal Communications Version 5.6, and is located in subdirectory \install\admin\distrib. It is an ASCII file that can be edited to suit your needs. Unwanted trace options should be flagged with a semicolon to be treated as a comment.

To verify that the correct options have been applied and are active, you may issue the **status** option as follows:

```
C:\>cstrace  status
   Current Active Trace:
   GROUP: 3270/5250/VT Emulator  (2)
   COMPONENT: Communication data  (1)
   FLAG: TCP/IP  (1)

   GROUP: 3270/5250/VT Emulator  (2)
   COMPONENT: Event  (3)
   FLAG: Keystroke  (10000)
```

The **cstrace save** and **cstrace format** options must include a full file specification to the Application Data Location specified for your installation. It is the directory where the configurations files are located.

To find out a parameter for a command-line trace, you can use the GUI to set up the trace, start the trace from GUI with all parameters selected as needed, then issue **cstrace status** from a command line. The output shows the equivalent command line parameters. Apply the reading of the output to the command line parameters of **cstrace**.

You may also invoke the Information Bundler using the command line interface:

```
pcspd /q
```

where `/q` suppresses the pop-up window asking for the registry keys to be included.

Part 3

Appendixes

A

Introduction to TCP/IP security

This appendix discusses basic network security techniques available with TCP/IP, and provides an overview of a number of solutions for addressing security issues in networks.

The field of network security in general and of TCP/IP security in particular is very wide, so this appendix concentrates on the most recent and most widely used security techniques. The following topics are covered:

- Basic concepts of cryptography and digital certificates
- Firewall concepts
- Virtual private network (VPN) and IPSec
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)

For more details on the concepts covered in this chapter, please see *TCP/IP Tutorial and Technical Overview*, GG24-3376.

Basic concepts of cryptography and digital certificates

If you are sending data in the clear over a network that is not completely under your control from the receiver to the sender, you will be unable to ensure the following security functions:

- **Privacy**

  Anyone who is able to intercept your data might be able to read it.

- **Integrity**

  An intermediary might be able to alter your data.

- **Accountability or non-repudiation**

  It may be impossible to determine the originator of a message with confidence, and thus the person who sent the message could deny being the originator.

Security functions such as identification and authentication are also impacted because if authentication data such as passwords are sent without integrity and privacy, they can be intercepted in transit between sender and receiver, making the authentication compromised and worthless.

To ensure privacy, integrity and accountability in non-secure networks, cryptographic procedures need to be used. Today, two distinct classes of encryption algorithms are in use: symmetric and asymmetric algorithms. They are fundamentally different in *how* they work, and thus in *where* they are used.

Symmetric encryption algorithms

An encryption algorithm is called symmetric because the same key that is used to encrypt the data is also used to decrypt the data and recover the clear text (see Figure A-1). The cipher and decipher processes are usually mathematically complex nonlinear permutations.

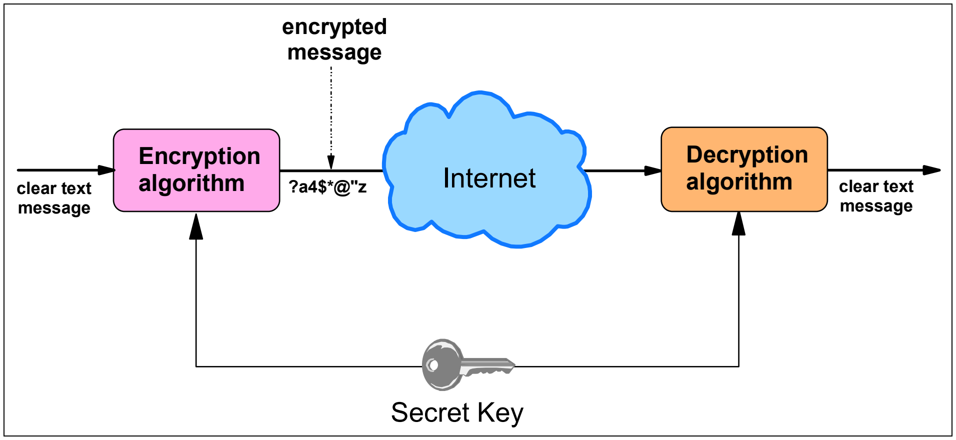


Figure A-1 Symmetric encryption and decryption: using the same key

Symmetric algorithms are usually efficient in terms of processing power, so they are ideal for encryption of bulk data. However, they have one major drawback, which is key management. The sender and receiver on any secure connection must share the same key; in a large network where thousands of users may need to communicate securely, it is extremely difficult to manage the distribution of keys so as not to compromise the integrity of any one of them.

Frequently used symmetric algorithms include:

- **Data Encryption Standard (DES)**

  Developed in the 1970s by IBM scientists, DES uses a 56-bit key. Stronger versions called Triple DES have been developed that use three operations in sequence: “2-key Triple DES” encrypts with key 1, decrypts with key 2, and encrypts again with key 1. The effective key length is 112 bits. “3-key Triple DES” encrypts with key 1, decrypts with key 2, and encrypts again with key 3. The effective key length is 168 bits.

- **Commercial Data Masking Facility (CDMF)**

  This is a version of the DES algorithm approved for use outside the U.S. and Canada (in times when export control was an issue). It uses 56-bit keys, but 16 bits of the key are known, so the effective key length is 40 bits.

- **RC2**

  Developed by Ron Rivest for RSA Data Security, Inc., RC2 is a block cipher with variable key lengths operating on 8-byte blocks. Key lengths of 40, 56, 64, and 128 bits are in use.

- **RC4**

  Developed by Ron Rivest for RSA Data Security, Inc., RC4 is a stream cipher operating on a bit stream. Key lengths of 40 bits, 56 bits, 64 bits, and 128 bits are in use. The RC4 algorithm always uses 128-bit keys; the shorter key lengths are achieved by “salting” the key with a known, non-secret random string.

- **Advanced Encryption Standard (AES)**

  As a result of a contest for a follow-on standard to DES held by the National Institute for Standards and Technology (NIST), the Rijndael algorithm was selected. This is a block cipher created by Joan Daemen and Vincent Rijmen with variable block length (up to 256 bits) and variable key length (up to 256 bits).

- **The International Data Encryption Algorithm (IDEA)**

  IDEA was developed by James Massey and Xueija Lai at ETH in Zurich. It uses a 128-bit key and is faster than triple DES.

DES is probably the most scrutinized encryption algorithm in the world. Much work has been done to find ways to break DES, notably by Biham and Shamir, but also by others. However, a way to break DES with appreciably less effort than a brute-force attack (breaking the cipher by trying every possible key) has not been found.

Both RC2 and RC4 are proprietary, confidential algorithms, which have never been published. They have been examined by a number of scientists under non-disclosure agreements.

With all the ciphers listed above, it can be assumed that a brute-force attack is the only means of breaking the cipher. Therefore, the work factor depends on the length of the key. If the key length is n bits, the work factor is proportional to 2**(n-1).

Today, a key length of 56 bits is generally only seen as sufficiently secure for applications that do not involve significant amounts of money or critically secret data. If specialized hardware is built (such as the machine built by John Gilmore and Paul Kocher for the Electronic Frontier Foundation), the time needed for a brute-force attack can be reduced to about 100 hours or less (see: *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design,* by Electronic Frontier Foundation, John Gilmore (Editor), 1988). Key lengths of 112 bits and above are seen as unbreakable for many years to come, since the work factor rises exponentially with the size of the key.

Asymmetric encryption algorithms

Asymmetric encryption algorithms are so called because the key that is used to encrypt the data cannot be used to decrypt the data; a different key is needed to recover the clear text (see Figure A-2). This key pair is called a public key and a private key. If the public key is used to encrypt the data, the private key must be used to recover the clear text. If data is encrypted with the private key, it can only be decrypted with the public key.

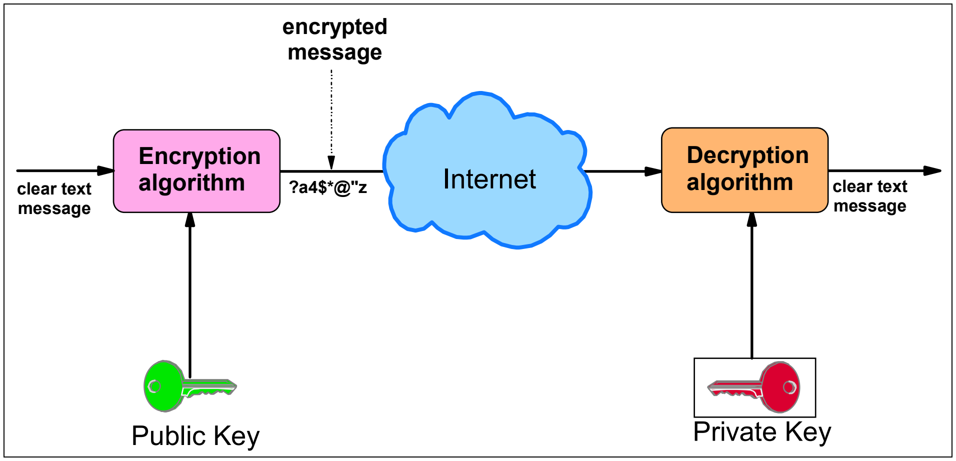


Figure A-2 Public-key cryptography: using a key pair

Asymmetric encryption algorithms, commonly called Public Key Cryptography Standards (PKCS), are based on mathematical algorithms. The basic idea is to find a mathematical problem that is very hard to solve. The algorithm in most widespread use today is RSA. However, some companies have begun to implement public-key cryptosystems based on elliptic curve algorithms. With the growing proliferation of IPSec, the Diffie-Hellman algorithm is gaining popularity.\

A brief overview of all three methods follows:

- **RSA**

  Invented 1977 by Rivest, Shamir, and Adleman (who formed RSA Data Security Inc.). The idea behind RSA is that integer factorization of very large numbers is extremely hard to do. Key lengths of public and private keys are typically 512 bits, 768 bits, 1024 bits, or 2048 bits. The work factor for RSA with respect to key length is sub-exponential, which means the effort does not rise exponentially with the number of key bits. It is roughly 2**(0.3*n).

- **Elliptic curve**

  Public-key cryptosystems based on elliptic curves use a variation of the mathematical problem of finding discrete logarithms. It has been stated that an elliptic curve cryptosystem implemented over a 160-bit field has roughly the same resistance to attack as RSA with a 1024-bit key length. Properly chosen elliptic curve cryptosystems have an exponential work factor (which explains why the key length is so much smaller). Elliptic curve cryptosystems are now standardized by FIPS PUB 186-2, the digital signature standard (January 2000).

- **Diffie-Hellman**

  W. Diffie and M.E. Hellman, the inventors of public key cryptography, published this algorithm in 1976. The mathematical problem behind Diffie-Hellman is computing a discrete logarithm. Both parties have a public-private key pair each; they are collectively generating a key only known to them. Each party uses its own private key and the public key of the other party in the key generation process. Diffie-Hellman public keys are often called *shares*.

The beauty of asymmetric algorithms is that they are not subject to the key management issues that beset symmetric algorithms. Your public key is freely available to anyone, and if someone wants to send you a message he or she encrypts it using that key. Only you can understand the message, because only you have the private key. Asymmetric algorithms are also very useful for authentication. Anything that can be decrypted using your public key must have been encrypted using your private key, in other words, by you.

Performance issues of cryptosystems

Elliptic curve cryptosystems are said to have performance advantages over RSA in decryption and signing. While the possible differences in performance between the asymmetric algorithms are somewhere in the range of a factor of 10, the performance differential between symmetric and asymmetric cryptosystems is far more dramatic.

For instance, it takes about 1000 times as long to encrypt the same data with RSA (an asymmetric algorithm) as with DES (a symmetric algorithm), and implementing both algorithms in hardware does not change the odds in favor of RSA.

As a consequence of these performance issues, the encryption of bulk data is usually performed using a symmetric cryptosystem, while asymmetric cryptosystems are used for electronic signatures, and in the exchange of key material for secret-key cryptosystems. With these applications, only relatively small amounts of data need to be encrypted and decrypted, and the performance issues are less important.

Cryptosystems for data integrity

Data integrity is the ability to assert that the data received over a communication link is identical to the data sent. Data integrity in an insecure network requires the use of cryptographic procedures. However, it does not imply that only the receiver is able to read the data, as with data privacy. Data can be compromised not only by an attacker, but also by transmission errors (although those are normally handled by transmission protocols such as TCP).

Message digest algorithms

A message digesting algorithm (often also called a “digital hash”) is an algorithm that “digests” (condenses) a block of data into a shorter string (usually 128 or 160 bits), which is called a message digest, secure hash, or Message Integrity Code (MIC). See Figure A-3 for a graphical representation. The principle behind message digest algorithms is as follows:

- The message cannot be recovered from the message digest.

It is very hard to construct a block of data that has the same message digest as another given block.

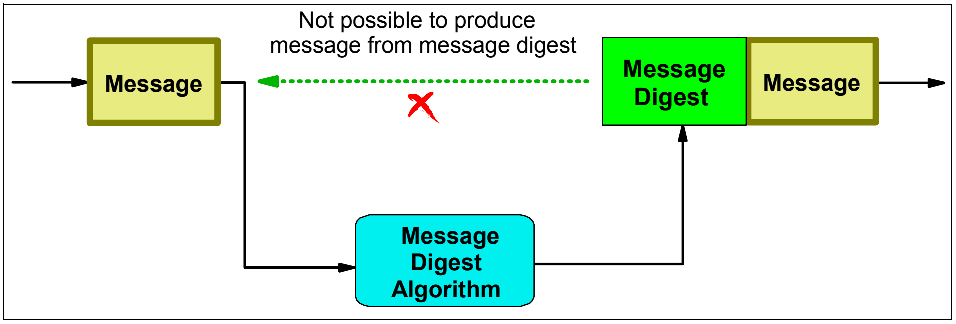


Figure A-3 Message digest

Common message digest algorithms are:

- **MD2**

  Developed by Ron Rivest of RSA Data Security, Inc. The algorithm is mostly used for Privacy Enhanced Mail (PEM) certificates. MD2 is fully described in RFC 1319. Since weaknesses have been discovered in MD2, its use is discouraged.

- **MD5**

  Developed in 1991 by Ron Rivest. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit message digest of the input. The MD5 message digest algorithm is specified in RFC 1321, *The MD5 Message-Digest Algorithm*. Collisions have been found in MD5; see *Cryptanalysis of MD5 Compress*, by Hans Dobbertin, available at:

  `http://www.cs.ucsd.edu/users/bsy/dobbertin.ps`

- **SHA-1**

  Developed by the National Security Agency (NSA) of the U.S. Government. The algorithm takes as input a message of arbitrary length and produces as output a 160-bit “hash” of the input. SHA-1 is fully described in standard FIPS PUB 180-1, also called the Secure Hash Standard (SHS). SHA-1 is generally recognized as the strongest and most secure message digesting algorithm.

- **SHA-256, SHA-512**

  Developed by the National Security Agency (NSA) of the U.S. Government. The security of a hash algorithm against collision attacks is half the hash size, and this value should correspond with the key size of encryption algorithms used in applications together with the message digest. Since SHA-1 only provides 80 bits of security against collision attacks, this is deemed inappropriate for the key lengths of up to 256 bits planned to be used with AES. Therefore, extensions to the Secure Hash Standard (SHS) have been developed. SHA-256 provides a hash size of 256 bits while SHA-512 provides a hash size of 512 bits.

Message digests for data integrity

The sender of a message (block of data) uses an algorithm, for example, SHA-1, to create a message digest from the message (see Figure A-4). The message digest can be sent together with the message to provide data integrity. The receiver runs the same algorithm over the message and compares the resulting message digest to the one sent with the message. If both match, the message is unchanged.

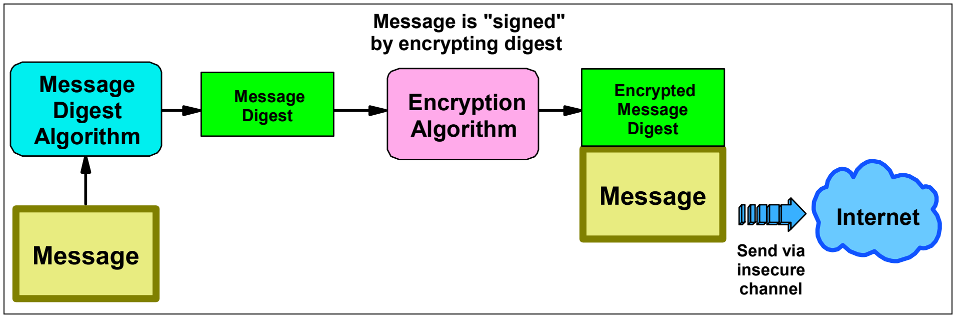


Figure A-4 Message digest for data integrity

The message digest should not be sent in the clear: Since the digest algorithms are well-known and no key is involved, a man-in-the-middle cannot only forge the message but also can replace the message digest with that of the forged message. This would make it impossible for the receiver to detect the forgery. The solution for this is to encrypt the message digest, that is, to use a message authentication code (MAC).

Message authentication codes

Secret-key cryptographic algorithms, such as DES, can be used for encryption with message digests. A disadvantage is that, as in secret-key cryptosystems, the keys must be shared by sender and receiver. Furthermore, since the receiver has the key that is used in MAC creation, this system does not offer a guarantee of non-repudiation. That is, it is theoretically possible for the receiver to forge a message and claim it was sent by the sender. Therefore, message authentication codes are usually based on public/private key encryption in order to provide for non-repudiation. This is discussed further in “Digital signatures” on page 1018.

Keyed hashing for message authentication (HMAC)

H. Krawczyk and R. Canetti of IBM Research and M. Bellare of UCSD invented a method to create a message authentication code called HMAC, which is defined in RFC 2104 as a proposed Internet standard. A simplified description of how to create the HMAC is as follows: The key and the data are concatenated and a message digest is created. The key and this message digest are again concatenated for better security, and another message digest is created, which is the HMAC.

HMAC can be used with any cryptographic hash function. Typically, either MD5 or SHA-1 are used. In the case of MD5, a key length of 128 bits is used (the block length of the hash algorithm). With SHA-1, 160-bit keys are used. Using HMAC actually improves the security of the underlying hash algorithm. For instance, some collisions (different texts that result in the same message digest) have been found in MD5. However, they cannot be exploited with HMAC. Therefore the weakness in MD5 does not affect the security of HMAC-MD5.

HMAC is now a PKCS#1 V.2 standard for RSA encryption (proposed by RSA Inc. after weaknesses were found in PKCS#1 applications). For further details, see:
http://www.ietf.org/rfc.html
HMAC is also used in the Transport Layer Security (TLS) Protocol, the successor to SSL.

Message authentication used with SSL

In the Secure Sockets Layer Protocol (SSL), a slightly different MAC algorithm has been implemented. The MAC write-secret and the sequence number of the message are concatenated with the data, and a message digest is created. The MAC write-secret and this message digest are again concatenated for better security, and another message digest is created, which is the MAC. Again, for the hash function, either MD5 or SHA-1 can be used. If compression is used, the text is compressed before the MAC is calculated.

Digital signatures

Digital signatures are an extension to data integrity. While data integrity only ensures that the data received is identical to the data sent, digital signatures go a step further: they provide non-repudiation. This means that the sender of a message (or the signer of a document) cannot deny authorship, similar to signatures on paper. As illustrated in Figure A-5, the creator of a message or electronic document that is to be signed uses a message digesting algorithm such as MD5 or SHA-1 to create a message digest from the data. The message digest and some information that identifies the sender are then encrypted with an asymmetric algorithm using the sender's private key. This encrypted information is sent together with the data.

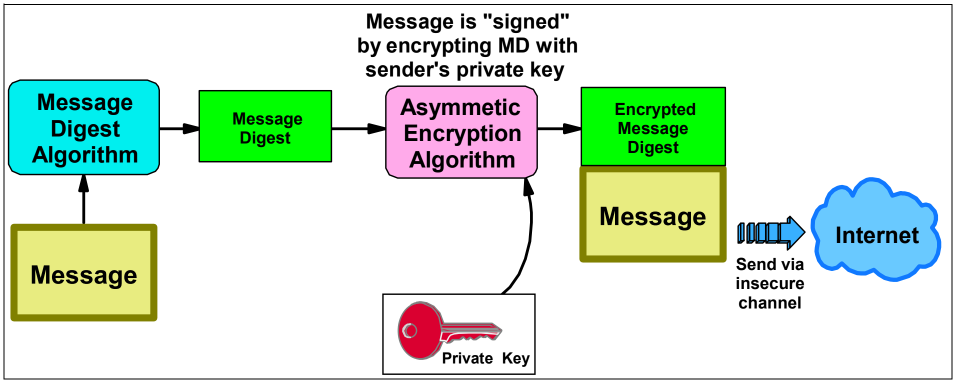


Figure A-5 Digital signature creation

The receiver, as shown in Figure A-6, uses the sender's public key to decrypt the message digest and identification of the sender. He or she will then use the message digesting algorithm to compute the message digest from the data. If this message digest is identical to the one recovered after decrypting the digital signature, the signature is recognized as valid proof of the authenticity of the message.

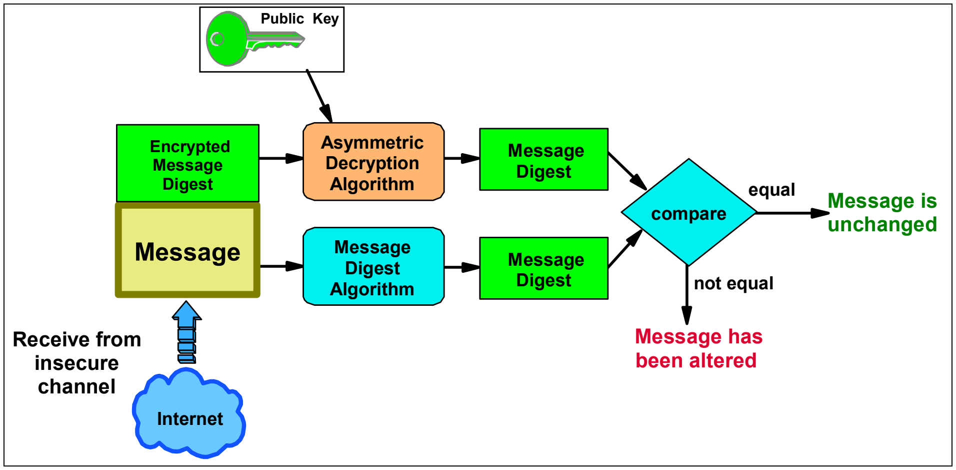


Figure A-6 Digital signature verification

With digital signatures, only public-key cryptosystems can be used. If secret-key cryptosystems are used to encrypt the signature, it is very difficult to make sure that the receiver (having the key to decrypt the signature) does not misuse this key to forge a signature of the sender. The private key of the sender is known to nobody else, so nobody is able to forge the sender's signature.

Note the difference between encryption using public-key cryptosystems and digital signatures:

- With encryption, the sender uses the receiver's public key to encrypt the data, and the receiver decrypts the data with his private key. This means everybody can send encrypted data to the receiver that only the receiver can decrypt. See Figure A-7 for a graphical representation.

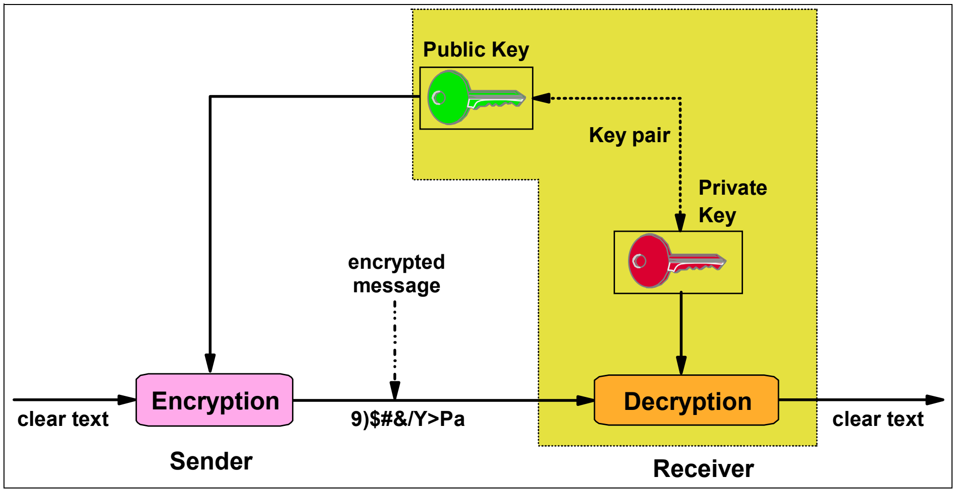


Figure A-7 Encrypting data with the receiver's public key

- With digital signatures, the sender uses his private key to encrypt his signature, and the receiver decrypts the signature with the sender's public key. This means that only the sender can encrypt the signature, but everybody who receives the signature can decrypt and verify it.

The tricky part with digital signatures is the trustworthy distribution of public keys, since a genuine copy of the sender's public key is required by the receiver. A solution to this problem is provided by digital certificates, which are discussed next.

Public Key Infrastructure

A Public Key Infrastructure (PKI) offers the basis for practical usage of public key encryption. A PKI defines the rules and relationships for certificates and Certificate Authorities (CAs). It defines the fields that can or must be in a certificate, the requirements and constraints for a CA in issuing certificates, and how certificate revocation is handled.

PKI has been exploited in many applications or protocols, such as Secure Sockets Layer (SSL), Secure Multimedia Internet Mail Extensions (S/MIME), IP Security (IPSec), Secure Electronic Transactions (SET), and Pretty Good Privacy (PGP). PKI is described here, only insofar as its use with Web serving and Secure Sockets Layer (SSL) is concerned. For more information on PKI, refer to *Deploying a Public Key Infrastructure*, SG24-5512.

Digital certificates

When using a PKI, the user must be confident that the public key belongs to the correct remote person (or system) with which the digital signature mechanism is to be used. This confidence is obtained through the use of public key digital certificates. A digital certificate is analogous to a passport: the passport certifies the bearer's identity, address, and citizenship. The concepts behind passports and other identification documents (for instance, drivers' licenses) are very similar to those that are used for digital certificates.

Passports are issued by a trusted authority, such as a government passport office. A passport will not be issued unless the person who requests it has proven their identity and citizenship to the authority. Specialized equipment is used in the creation of passports to make it very difficult to alter the information in it, or to forge a passport altogether. Other authorities, for instance, the border police in other countries, can verify a passport's authenticity. If they trust the authority that issued the document, they implicitly trust the passport.

A digital certificate serves two purposes: it establishes the owner's identity and it makes the owner's public key available. Similar to a passport, a certificate must be issued by a trusted authority, the CA; and, like a passport, it is issued only for a limited time. When its expiration date has passed, it must be replaced.

Trust is a very important concept in passports, as well as in digital certificates. In the same way as, for instance, a passport issued by the governments of some countries, even if recognized to be authentic, will probably not be trusted by the US authorities, each organization or user has to determine whether a CA can be accepted as trustworthy.

For example, a company might want to issue digital certificates for its own employees from its own Certificate Authority; this could ensure that only authorized employees are issued certificates, as opposed to certificates being obtained from other sources such as a commercial entity such as VeriSign.

The information about the certificate owner's identity is stored in a format that follows RFC 2253 and the X.520 recommendation, for instance: CN=Juan Shaughnessy O=IBM Corporation; the complete information is called the owner's distinguished name (DN). The owner's distinguished name and public key and the CA's distinguished name are digitally signed by the CA; that is, a message digest is calculated from the distinguished names and the public key. This message digest is encrypted with the private key of the CA.

Figure A-8 shows the layout of a digital certificate.

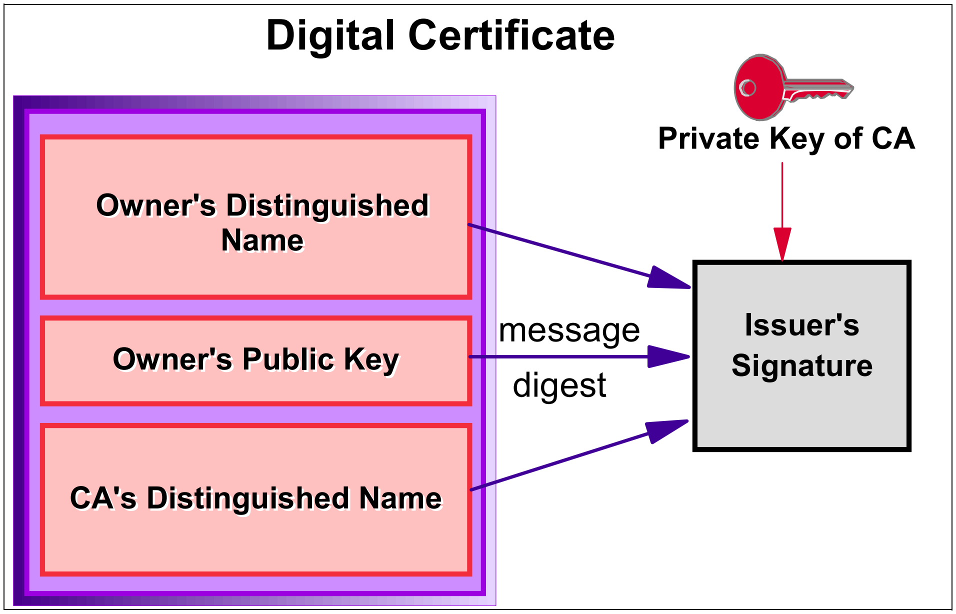


Figure A-8 Simplified layout of a digital certificate

The digital signature of the CA serves the same purpose as the special measures taken for the security of passports such as laminating pages with plastic material; it allows others to verify the authenticity of the certificate. Using the public key of the CA, the message digest can be decrypted. The message digest can be recreated; if it is identical to the decrypted message digest, the certificate is authentic.

Security considerations for certificates

If I send my certificate with my public key in it to someone else, what keeps this person from misusing my certificate and posing as myself? The answer is the private key.

A certificate alone can never be proof of anyone's identity. The certificate just allows the identity of the certificate owner to be verified by providing the public key that is needed to check the certificate owner's digital signature. Therefore, the certificate owner must protect the private key that matches the public key in the certificate. If the private key is stolen, the thief can pose as the legitimate owner of the certificate. Without the private key, a certificate cannot be misused.

An application that authenticates the owner of a certificate cannot accept just the certificate. A message signed by the certificate owner should accompany the certificate. This message should use elements such as sequence numbers, time stamps, challenge-response protocols, or other data that allow the authenticating application to verify that the message is a "fresh" signature from the certificate owner and not a replayed message from an impostor.

Certificate Authorities and trust hierarchies

A user of a security service requiring knowledge of a public key generally needs to obtain and validate a certificate containing the required public key. To verify that the certificate is authentic, the receiver needs the public key of the CA that issued the certificate.

Most Web browsers come configured with the public keys of common CAs (such as VeriSign). However, if the user does not have the public key of the CA that signed the certificate, an additional certificate is needed in order to obtain that public key. In general, a chain of multiple certificates may be required, comprising a certificate of the public key owner signed by a CA, and possibly additional certificates of CAs signed by other CAs. Many applications that send a subject's certificate to a receiver send not only just that certificate, but also all the CA certificates necessary to verify the certificate up to the root.

Obtaining and storing certificates

As has been discussed, certificates are issued by a CA. Clients usually request certificates by going to the CA's Web site. After verifying the validity of the request, the CA sends back the certificate in an e-mail message, or allows it to be downloaded.

Requesting server certificates

Server certificates can be either self-signed or they can be signed by an external CA. The server environment will determine which kind of certificate should be used. In an intranet environment, it is generally appropriate to use self-signed certificates. In an environment where external users are accessing the server over the Internet, it is usually advisable to acquire a server certificate from a well-known CA, because the steps needed to import a self-signed certificate might seem obscure, and most users will not have the ability to discern whether the action they are performing is of trivial consequence or not. It should also be noted that a root CA certificate received over a channel that is not trusted, such as the Internet, does not deserve any kind of trust.

Firewall concepts

A firewall machine is a computer used to separate a secure network from a non-secure network (Figure A-9). Such networks are typically based on the TCP/IP protocol, but the concept of a firewall is not restricted to just TCP/IP.

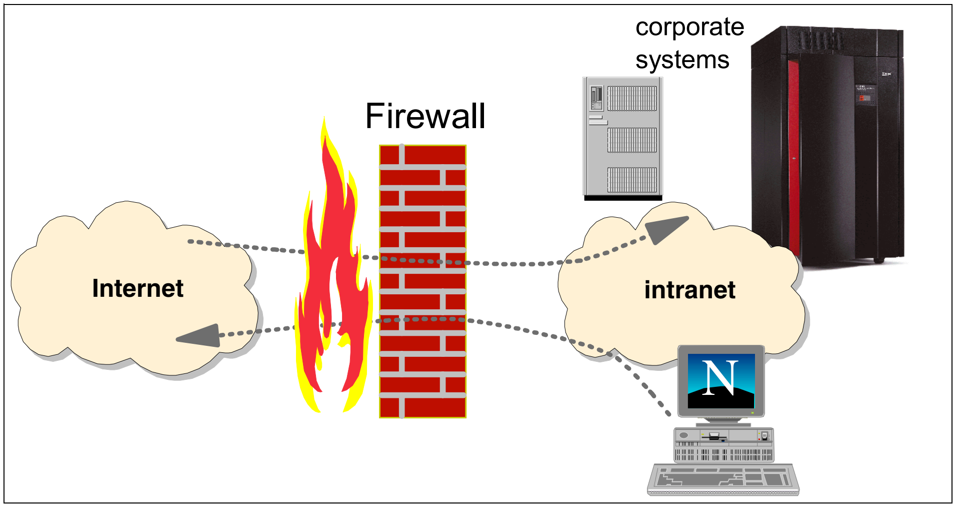


Figure A-9 The firewall concept

Firewalls have become an important concept in TCP/IP-based networks, because the global Internet is a TCP/IP-based network, and is often perceived as being a non-secure place to enter or traverse. Yet, you still want your intranet (perceived as being a secure place) to be connected to the non-secure Internet.

The reasons for establishing connections between an intranet and the Internet are many, but generally fall into two categories:

- You want to provide a service to the Internet community or want to conduct business on the Internet.
- You want to allow your internal employees to access the vast amount of services on the Internet, as well as the ability to exchange or share information with other users on the Internet or through the Internet.

At this point, it might be useful to define the following terms:

- The term *intranet* refers to an internal TCP/IP network.
- The term *Internet* refers to the World Wide Web, and the associated infrastructure of news groups, e-mail, chat rooms, and other services.
- The term *extranet* refers to TCP/IP networks of different companies connected with a secure connection, perhaps using virtual private network technology (VPN).

Doing e-business on the Internet is very different from just serving static information out of a Web server. Doing e-business means that you have to establish an environment where users on the Internet are able to interact with the applications and data that your daily existence as a company is based on and relies upon.

That data and those applications are likely, to a large extent, to be located in your environment, which means that you probably already are, or in the near-term future will be, challenged with the request to establish Internet access to your production environment.

When you connect your intranet to the Internet and define a strategy for how your firewall should function, you may think that it is sufficient to block all types of traffic that represent a risk, and allow the remaining traffic to pass through the firewall. However, such a strategy is based on the assumption that all risks are known in advance and that existing well-behaving traffic will remain well-behaving; such an assumption is a mistake. New ways of exploiting existing applications and well-known application protocols are being found every week, so an application that may be considered harmless today may be the instrument of an attack tomorrow.

General guidelines for implementing firewalls

A few general guidelines for implementing firewall technologies are worth including.

Before you start connecting your intranet to the Internet, define a security policy for how your firewall should function and how demilitarized zones should be configured. Decide what type of traffic is allowed through the firewall, and under what conditions, what kind of servers are to be placed in demilitarized zones, and what type of traffic is allowed between the demilitarized zone and the intranet.

When actually configuring your firewall, start by disallowing everything and then proceed by enabling those services you have defined in your security policy. Everything that is not specifically allowed should be prohibited.

If you establish more than a single gateway between your internal network and the Internet, make sure that all gateways implement the same level of security. It is common practice to use different firewall products in a vertical setup (product A between the Internet and the demilitarized zone and product B between the demilitarized zone and the intranet). That way, a hacker exploiting a vulnerability in product A is still stopped by product B. Of course, it does not make sense to use this concept in a horizontal setup (one gateway uses product A, the other one product B) because a hacker will get in at the weakest link.

If you build a perfect firewall on one end of your network while users on the other end dial in to the Internet from their LAN-attached PCs, enabling those PCs to act as IP routers between your internal network and the Internet, a hacker is soon going to exploit that back door into your network instead of wasting his time trying to break through your firewall.

One of the most important aspects of a firewall is its ability to log both successful and rejected access events. However, these logs are worth nothing if you do not set up daily administrative procedures to analyze and react to the information that can be derived from these logs.

By analyzing the firewall logs, you should be able to detect if unauthorized accesses were attempted and if your firewall protection succeeded in rejecting such attacks, or if it failed and allowed an intruder to gain access to resources that should not have been accessed. In addition, it might be a good idea to install an intrusion detection system.

This list is not all-inclusive, but merely points out some of the most important aspects of implementing firewall technologies in your network.

So far, the Internet has been considered to be the non-secure place, while your internal network has been considered the secure place. However, that may in some situations be an oversimplification. For example, consider a research department that works with highly confidential information. In such an environment, you may want to protect that research department from your regular users by implementing a firewall between your regular internal network and the network in your research department.

Firewall categories

There are many firewall technologies available, but they can in general be grouped into two major categories:

- Those that allow IP packets to be routed between two or more networks, namely packet-filtering routers.

- Those that disable IP routing, but relay data through specialized application programs, namely application-level gateways or proxies.

Packet filtering

A packet filtering router, as shown in Figure A-10, is a special type of IP router. What differentiates a firewall packet filtering router from a normal IP router is that it applies one or more technologies to analyze the IP packets and decide if a packet is allowed to flow through the firewall or not. Such a firewall is sometimes also referred to as a screening filter, or router firewall.

Some packet-filtering techniques only act on data in the headers of individual packets, while others also look at data depending on the type of packet. The traditional packet-filtering router is stateless (each packet is handled independently) but there are products that save state over multiple packages and base their actions on the state information.

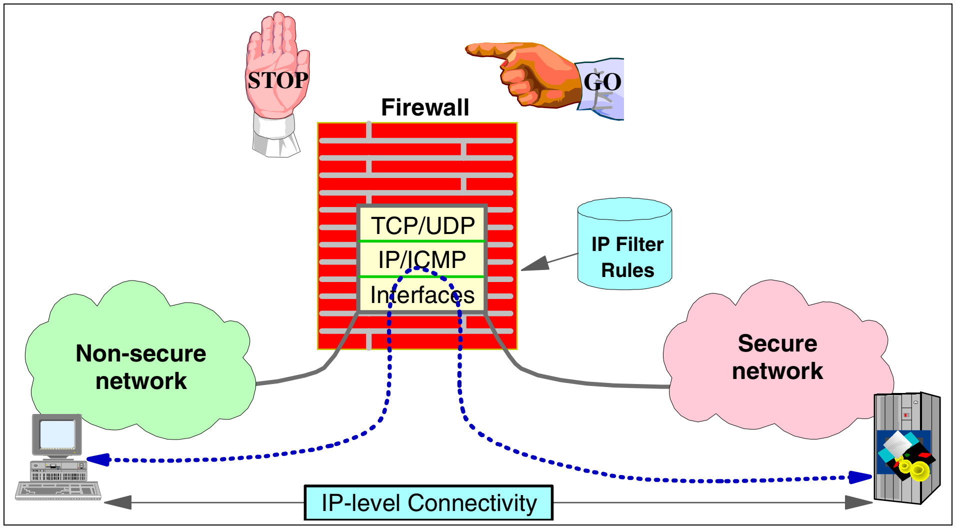


Figure A-10 Packet filtering firewall

Application-level gateway

An application-level gateway, sometimes referred to as a bastion host, is a machine that disables IP-level routing between the non-secure network and the secure network, but allows specialized application gateway programs (termed proxies) that run on the firewall to communicate with both the secure network and the non-secure network. See Figure A-11.

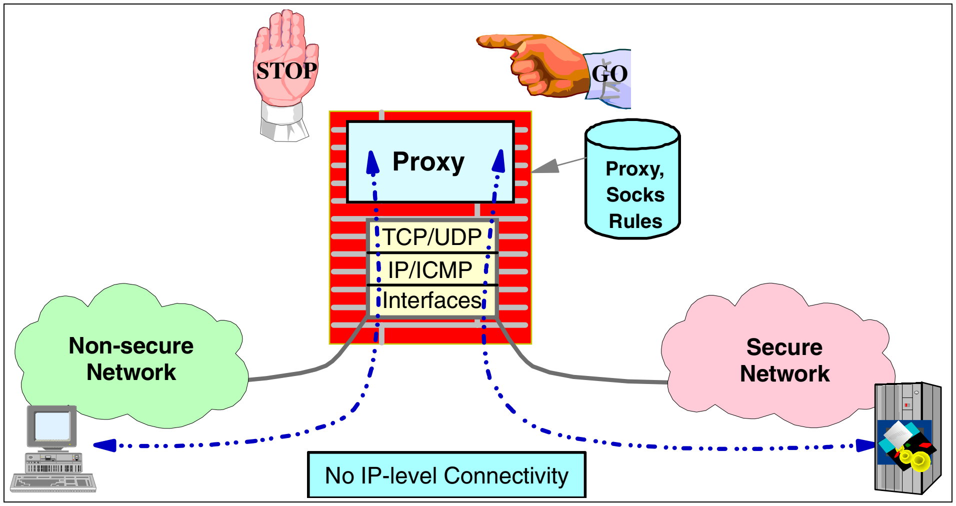


Figure A-11 Application gateway firewall

The proxy applications on the firewall act as relay applications between users or applications on the secure and the non-secure networks. Examples of such proxy applications are HTTP or FTP proxy servers. The SOCKS server is also an application-level gateway, but a special kind, sometimes referred to as a circuit level gateway. A SOCKS server can relay all TCP and UDP connections, not just HTTP or FTP sessions. It does not provide any extra packet processing or filtering, and unlike proxy servers, it is often used for outbound connections through a firewall.

A firewall may not always have to be configured as either a packet-filtering router or as a proxy; it may be configured to perform the following functions:

- IP filtering
- Network address translation (NAT)
- Virtual private networks (VPN)
- FTP proxy server
- SOCKS server
- Domain name services

An excellent discussion of firewall technologies can be found in *TCP/IP Tutorial and Technical Overview*, GG24-3376.

The demilitarized zone

The demilitarized zone (DMZ) is a term often used when describing firewall configurations. Figure A-12 shows a typical example. A DMZ is an isolated subnet between your secure network and the Internet. Much as the no-man's land between two entrenched armies, anyone can enter it, but the only things present are those that you want to allow access to anyway. Nowadays, a demilitarized zone is an area in which you place the Web servers and other servers for public access, but which you also wish to protect to some degree.

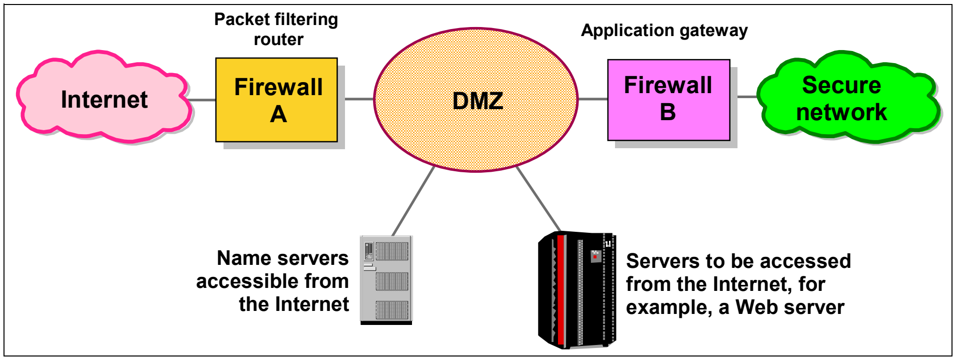

Packet filtering router
Application gateway
Internet
Firewall A
DMZ
Firewall B
Secure network
Name servers accessible from the Internet
Servers to be accessed from the Internet, for example, a Web server

Figure A-12 A demilitarized zone

This is achieved by placing an outer firewall (often a packet-filtering router) between the Internet and the servers in the DMZ, and another firewall (often an application-level gateway) between your secure network and the DMZ. The outer firewall is designed to allow into the DMZ only those requests you wish to receive at your Web servers, but could also be configured to block denial-of-service attacks and to perform network address translation of the servers in your DMZ. The inner firewall is designed to prevent unauthorized access to your secure network from the DMZ and also perhaps to prevent unauthorized access from your secure network to the DMZ or the connected non-secure network.

When you put a server into a DMZ, it is strongly recommended that you use firewall technologies. You should use firewall technologies to block all traffic into and out of your server that does not belong to the services you are going to offer from this server. This control should be in place even if you already have a packet-filtering router or firewall between the insecure network and this server.

Hardening

Hardening is a process done to firewalls to make them more secure. All unnecessary services, user accounts, and software on the operating system are removed or disabled.

An operating system is designed to fit computers with different configurations doing different tasks. To accomplish this, extra items are installed with the operating system that will only be used in certain situations. Much of the time, these extra items just take up resources and might cause the computer to run slower. On a firewall, these items become more of a problem. They become unnecessary, and potential security exposures.

Almost everything on a firewall is a potential security exposure. By disabling and removing the unnecessary items, there will be less exposure for a hacker to exploit. All services, user IDs, and software on a firewall should be required only by the operating system or the firewall. Everything else should be removed.

Many firewalls will perform a limited amount of hardening. However, it is the responsibility of the firewall administrator to finish the task.

Virtual private network (VPN) and IPSec

A virtual private network (VPN) provides secure connections across the Internet, by establishing a “tunnel” between two secure networks. It is a generic solution that is application and protocol-independent. A VPN encapsulates the IP datagram into another IP datagram in order to maintain data privacy. It can be used by two disparate parts of a corporation to connect their internal private networks by means of a non-secure network such as the Internet. An example of a VPN configuration is shown in Figure A-13.

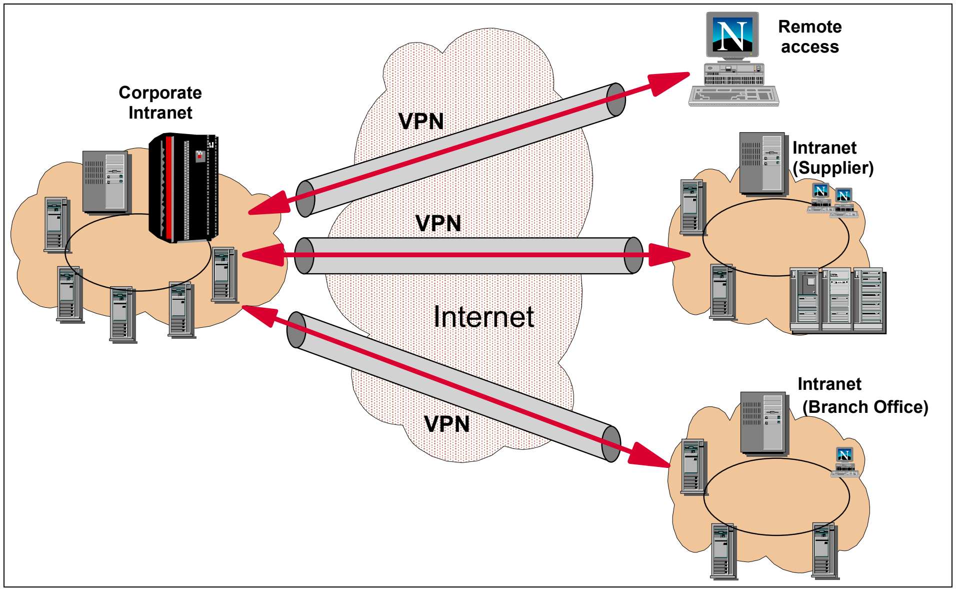


Figure A-13 Virtual private networks

IPSec

In Figure A-14 the TCP/IP layered protocol stack is shown, with the security-related protocols associated with each layer:

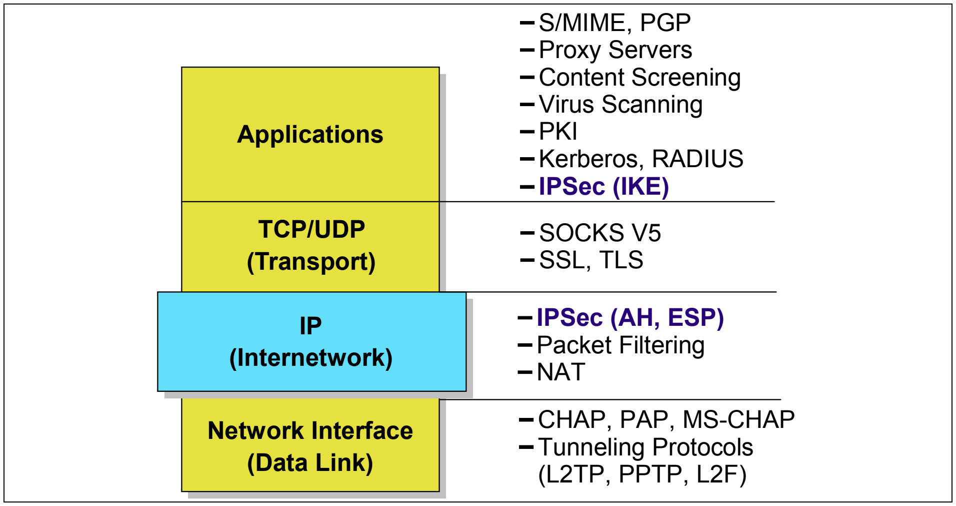


Figure A-14 The TCP/IP protocol stack and the security-related protocols

Within the layered communications protocol stack model, the network layer (IP in the case of the TCP/IP stack) is the lowest layer that can provide end-to-end security. Network-layer security protocols provide blanket protection for all upper-layer application data carried in the payload of an IP datagram, without requiring a user to modify the applications.

The IP Security Architecture (IPSec) open framework is defined by the IPSec Working Group of the IETF. IPSec is called a framework because it provides a stable, long-lasting base for providing network layer security. It can accommodate today's cryptographic algorithms, and can also accommodate newer, more powerful algorithms as they become available. IPv6 implementations must support IPSec, and IPv4 implementations are strongly recommended to do so.

IPSec is comprised of a number of components described in individual RFCs that are designed to operate together:

- Security Protocols: IP Authentication Header (AH) provides data origin authentication, data integrity, and replay protection, while IP Encapsulating Security Payload (ESP) provides data confidentiality, data origin authentication, data integrity, and replay protection.
- Security Associations: An SA is a kind of session between two hosts defining the protocols to be used when transmitting data. Internet Security Association and Key Management Protocol (SAKMP) is a generic framework for negotiating SAs and keys.
- Key Management: Internet Key Exchange (IKE) provides a method for automatically setting up security associations, and managing and exchanging their cryptographic keys.

Security Associations

An IPSec Security Association (SA) corresponds to a session between two hosts. It defines the set of protocols and, with these, the negotiated algorithms and keys that are to be used when transmitting data between two hosts. An SA for data traffic is always unidirectional, so for a pair of hosts that are to communicate securely, at least two SAs, one for each direction, are needed. This differs from other protocols that make use of sessions such as SSL for instance. An SSL session covers the transmission in both directions.

Negotiating Security Associations (ISAKMP and IKE)

Before any data can be sent between two hosts using IPSec, a SA needs to be established. The IPSec architecture provides two methods for establishing an SA: a manual tunnel or ISAKMP/IKE.

With manual tunnels, the SA and keying material are generated on one of the hosts (the tunnel owner), transferred to the other host (the tunnel partner) with an out-band transport mechanism, and then imported. This procedure needs to be repeated whenever the validity of the keys has expired, and new keying material needs to be generated.

Contrary to manual tunnels, ISAKMP and IKE provide automatic management of sessions and keys. ISAKMP provides a generic framework for the negotiation of SAs and keying material. It defines the procedures and packet formats to establish, negotiate, modify, and delete SAs, but it does not provide any specific key-generation techniques or cryptographic algorithms.

Internet Key Exchange (IKE) is based on two protocols: Oakley (*The Oakley Key Determination Protocol*, by H. Orman; RFC 2412, November 1998) and SKEME (*SKEME: A Versatile Secure Key Exchange Mechanism for the Internet*, by H. Krawczyk; IEEE Proceedings, 1996). For the key exchange, Diffie-Hellman (DH) shares are used and the shared key thus obtained is used to derive the keys for data encryption and message authentication. Authentication can be performed with one of three alternatives:

- Digital signatures
- Public key encryption
- A shared secret (a key previously known to both parties)

The use of DH shares causes the connection to have a property called “perfect forward secrecy.” This means that even if the keys for one session are completely compromised, the keys for previous sessions are still safe.

Phases: It takes two

Two hosts can communicate with each other in many different ways that may need different sorts of protection. For instance, some traffic may need encryption and authentication, while other traffic may only need authentication.

IKE uses a two-phase approach to be able to meet these different needs with minimal overhead. In phase 1, an ISAKMP SA is negotiated to create a secure, authenticated channel between the two hosts. The ISAKMP SA is a single, bidirectional security association. In phase 2, the SAs for the individual type of traffic (one SA for each direction) are negotiated using the authenticated channel established in phase 1.

Due to the Diffie-Hellman key exchange and the authentication, phase 1 is computationally rather expensive. Phase 2 does not involve key exchange nor authentication, and is much less expensive. Performing phase 1 just once for a pair of hosts and then multiple phase 2 operations for the individual connections is a concept that can improve performance considerably.

Identity protection

In phase 1, certificates and authentication data are exchanged between the hosts. IKE offers *identity protection*, meaning that all information that could identify a host to an attacker or eavesdropper can be encrypted. Depending on whether identity protection is really required, IKE supports two modes for phase 1: *main mode* offers identity protection, while *aggressive mode* does not. In main mode, a shared, secret key is established before the identification information (for instance, the host's digital certificate) is sent. For a diagram showing IKE main mode, see Figure A-15.

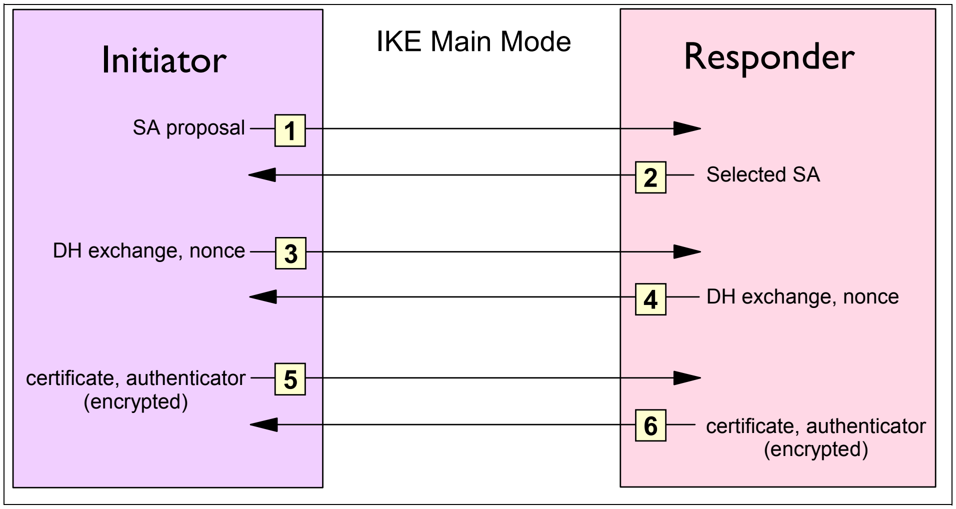


Figure A-15 IKE phase 1 main mode

Aggressive mode does not require the DH key exchange to be completed before sending the remaining information. Therefore, there is only one exchange of messages in aggressive mode (see Figure A-16).

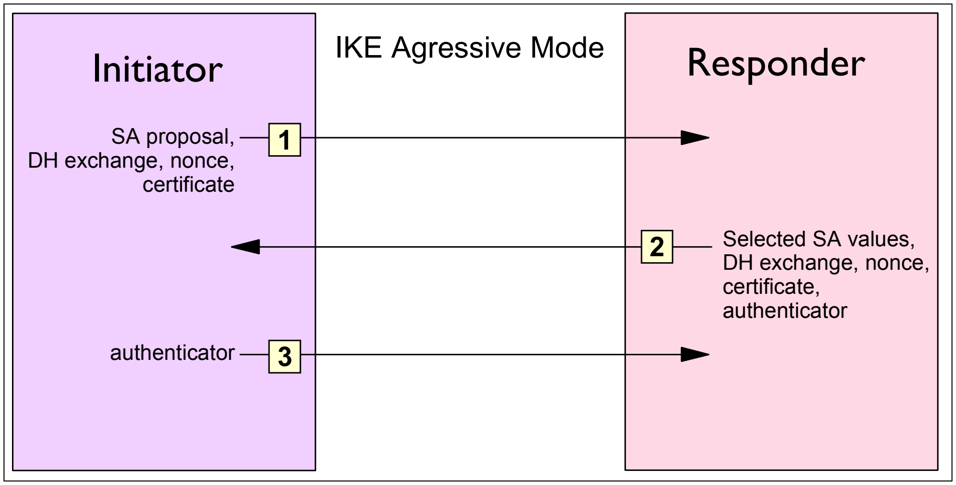


Figure A-16 IKE phase 1 aggressive mode

The exchange of messages taking part in phase 2 (negotiation of the SAs for the individual type of traffic) is called *quick mode*. In this mode, the pair of SAs for the intended type of communication is set up. The required keys for encryption and message authentication are generated from the shared key obtained in phase 1.

Transmitting data with IPSec

When a host wants to transmit one or more packets to another host it had not contacted before, it will perform the necessary IKE exchanges to set up the required SAs with the other hosts. Once this has all been performed and the necessary keys are generated, the host proceeds to send the first packet.

IPSec has two formats for sending data, which serve slightly different purposes. *Authentication Header* (AH) provides for message authentication and replay protection, whereas *Encapsulating Security Payload* (ESP) provides for data encryption in addition to message authentication and replay protection. The SA for a communication selects whether AH, ESP, or a combination of both is to be used.

Depending on the type of VPN connection between the two hosts, there are two modes, *tunnel mode* and *transport mode*, which are to be used.

ESP and AH in transport mode

If a VPN connection is being established between two hosts that are the endpoints for the packets transmitted between them, transport mode should be used. Figure A-17 shows the format of an Authentication Header (AH) in transport mode.

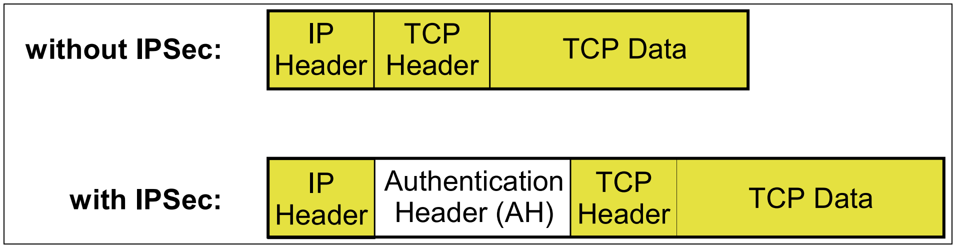


Figure A-17 AH in transport mode

The message authentication applied by AH protects the parts of the packet that are shaded in Figure A-17. Note that although the IP header is shaded in the diagram, parts of it are not authenticated because they can change in transit between sender and receiver.

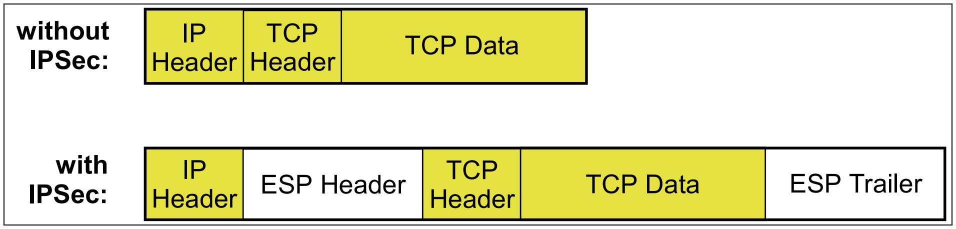


Figure A-18 ESP in transport mode

With the Encapsulating Security Payload (ESP) format in transport mode, the TCP header and data are encrypted and, optionally, authenticated. But as can be seen in Figure A-18 (the protected areas are shaded), the IP header is afforded no protection at all. However, this should not be a problem because sending and receiving hosts have been authenticated and verified in the SA.

ESP in tunnel mode

A common application of VPNs is the use of a protected tunnel between two secure networks. IPSec-capable firewalls at each end of the tunnel encrypt the packets they send from the secure network through the tunnel; they decrypt the packets they receive from the tunnel and route them to the destination hosts. In this scenario, the SAs do not authenticate the destination hosts (just the firewalls) and an attacker's modification of the IP headers could go undetected.

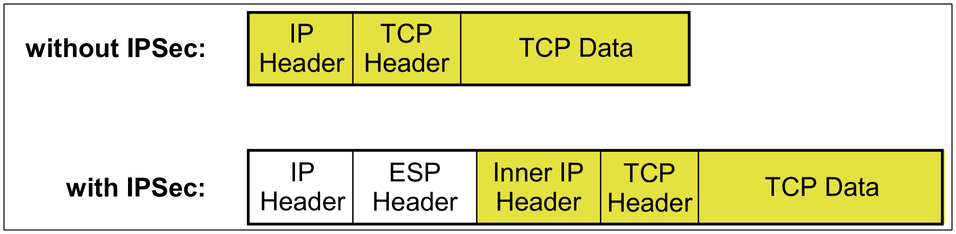


Figure A-19 ESP in tunnel mode

In this environment, tunnel mode is to be used. Figure A-19 shows the format of ESP packets in this mode; again, protected areas are shaded. The complete original packet, including the original IP header, is used as payload for an ESP packet. The inner IP header has the address of the destination host while the outer IP header addresses the firewall at the end of the tunnel. In this way, the complete packet including the IP header is protected.

In some cases, the AH and ESP formats are combined (applied one after the other) in order to reap both the benefits of IP header authentication with AH and payload (data) encryption with ESP.

For detailed information, read:

- *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201
- *Secure e-business in TCP/IP Networks on OS/390 and z/OS*, SG24-5383

Alternative VPN solutions: Layer 2 tunnel protocol

A remote access dial-up solution for mobile users is a very simple form of a virtual private network, typically used to support dial-in access to a corporate network whose users are all company employees. To eliminate the long-distance charges that would occur if a remote user were to dial in directly to a gateway on the home network, the IETF developed a tunneling protocol, Layer 2 Tunnel Protocol (L2TP). This protocol extends the span of a PPP connection: instead of beginning at the remote host and ending at a local ISP's point of presence, the virtual PPP link now extends from the remote host all the way back to the corporate gateway. In effect, the remote host appears to be on the same subnet as the corporate gateway.

Since the host and the gateway share the same PPP connection, they can take advantage of PPP's ability to transport protocols other than just IP. For example, L2TP tunnels can be used to support remote LAN access as well as remote IP access. Figure A-20 outlines a basic L2TP configuration:

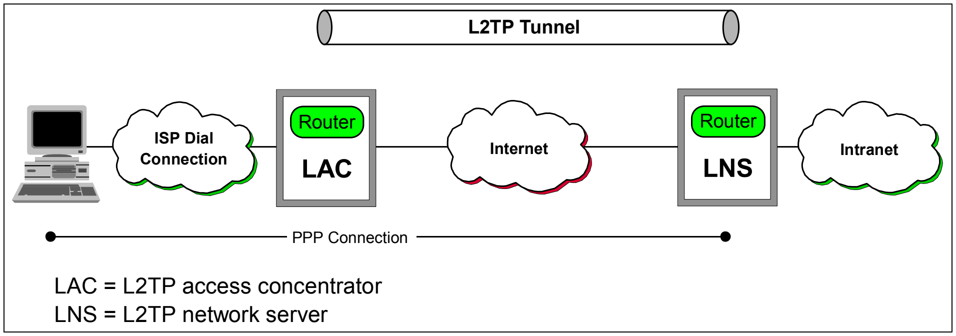


Figure A-20   Layer 2 Tunnel Protocol (L2TP) scenario

Although L2TP provides cost-effective access, multi-protocol transport, and remote LAN access, it does not provide cryptographically robust security features. For example:

- Authentication is provided only for the identity of tunnel endpoints, but not for each individual packet that flows inside the tunnel. This can expose the tunnel to various attacks.
- Without per-packet integrity, it is possible to mount denial-of-service attacks by generating bogus control messages that can terminate either the L2TP tunnel or the underlying PPP connection.
- L2TP itself provides no facility to encrypt user data traffic. This can lead to embarrassing exposures when data confidentiality is an issue.
- While the payload of the PPP packets can be encrypted, the PPP protocol suite does not provide mechanisms for automatic key generation or for automatic key refresh. This can lead to someone listening in on the wire to finally break that key and gain access to the data being transmitted.

Secure Sockets Layer

Secure Sockets Layer (SSL) is a protocol developed by the Netscape Communications Corporation that uses encryption to provide privacy and authentication between two applications using TCP/IP. SSL can be regarded as a *transport layer* equivalent of IPSec. Like IPSec, it uses asymmetric cipher algorithms (RSA is normally used) to authenticate users and sign messages, and symmetric algorithms to ensure confidentiality. Unlike IPSec, it is used to protect sessions between particular applications on particular ports; IPSec provides blanket protection between two hosts.

HTTP can use SSL to secure its communications. This allows Web browsers and servers to pass confidential or sensitive data through the Internet or intranet. SSL is also implemented by the Lightweight Directory Access Protocol (LDAP) for secure connections between LDAP clients and LDAP servers, by Telnet, and by a Telnet client such as Host On-Demand for connections between the client and the host system.

SSL overview

SSL was originally developed to protect traffic between a client and a server communicating across the Internet. The latest version of SSL from Netscape (and final version from Netscape) is SSL 3.0. At time of writing, it is by far the most commonly used SSL protocol. According to the latest SSL standard (RFC 2246, *The TLS Protocol Version 1.0*) SSL 2.0 should be phased out "with all due haste." The IETF TLS-Based Telnet Security document (see "Transport Layer Security Protocol (TLS)" on page 1043) goes a step further to say that SSL 2.0 is not an acceptable protocol at all. See Figure A-21 on page 1040 for an outline of some of the SSL protocols and standards.

The use of SSL for Web access is through a protocol called HTTPS. HTTPS is a unique protocol that combines SSL and HTTP. You need to specify https:// instead of `http://` as an anchor in HTML documents that link to SSL-protected documents. A client user can also open a URL by specifying `https://` to request SSL-protected documents.

Because HTTPS and HTTP are different protocols and use different ports (the default ports are 443 and 80, respectively), you can run both SSL and non-SSL requests at the same time. As a result, you can elect to provide information to all users using no security, and specific information only to browsers that make secure requests. This is how a retail company on the Internet can allow users to look through the merchandise without security, but then fill out order forms and send their credit card numbers using security.

SSL relies on digital certificates and a hierarchy of trusted authorities, as described in "Digital certificates" on page 1021, to ensure authentication of clients or servers.

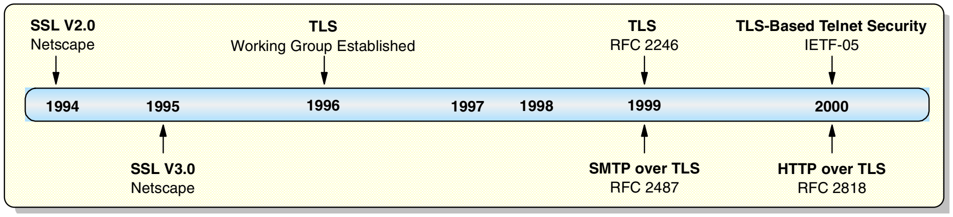


Figure A-21 Evolution of SSL

Establishing secure communications with SSL

To use SSL, both the client and the server need to have the software to support this protocol. Because SSL started with HTTP communication, it is used as an illustration.

The latest Netscape and Microsoft browsers support SSL 3.0 and all its features on the client. SSL is composed of two sub-protocols:

- SSL Handshake Protocol
- SSL Record Protocol

The SSL Handshake Protocol initializes a secure session, with authentication of the server (and optionally, the client), agreement of encryption scheme, and transfer of encryption keys. A public-key algorithm, usually RSA, is used for the exchange of the symmetric encryption key and for digital signatures. With the server certificate, the client is also able to verify the server's identity. With SSL Version 3.0, the possibility of authenticating the client identity by using client certificates in addition to server certificates was added. The overall flow of these steps is shown in Figure A-22.

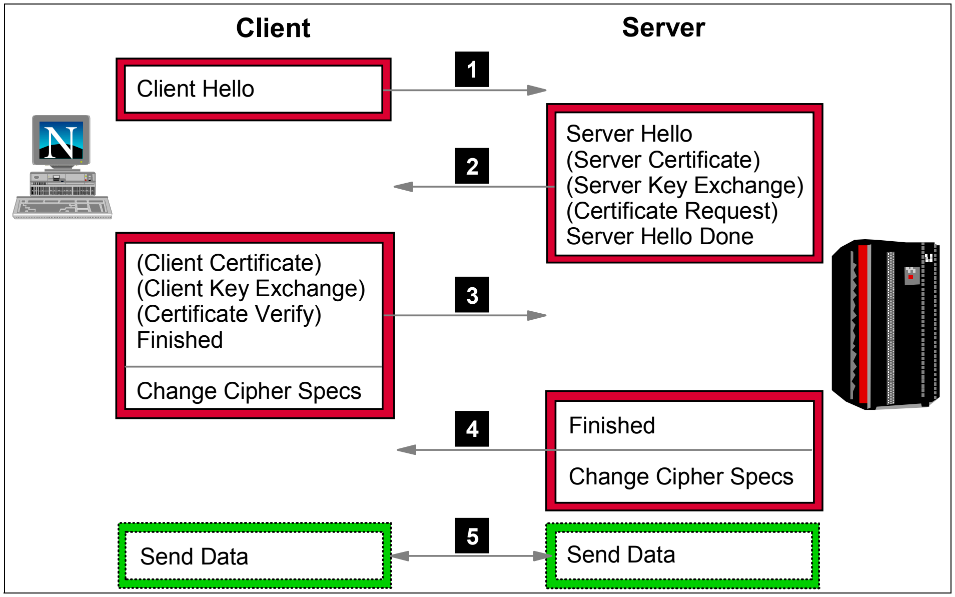


Figure A-22 Overview of SSL Handshake Protocol

- Step 1: The client sends a connection request with a `client hello` message. This message includes:
  - Desired version number
  - Time information (the current time and date in standard UNIX 32-bit format)
  - Optionally session-ID. If it is not specified the server will try to resume previous sessions or return an error message.
  - Cipher suites. (List of the cryptographic options supported by the client. These are authentication modes, key exchange methods, encryptions and MAC algorithms.)
  - Compression methods supported by the client
  - A random value (nonce). A nonce is a random value used in communication protocols, typically for replay protection.
- Step 2: The server evaluates the parameters sent by the `client hello` message and returns a `server hello` message that includes the following parameters which were selected by the server to be used for the SSL session:
  - Version number
  - Time information (the current time and date in standard UNIX 32-bit format)
  - Session ID
  - Cipher suite

- Compression method
- A random value

Following the `server hello` message, the server sends the following messages:

- Server certificate if the server is required to be authenticated
- A server key exchange message if there is no certificate available or the certificate is for signing only
- A certificate request if the client is required to be authenticated

Finally, the server sends a `server hello done` message and begins to wait for the client response.

- Step **3**: The client sends the following messages:
  - If the server has sent a certificate request, the client must send a certificate or a `no certificate` message.
  - If the server has sent a server key exchange message, the client sends a client key exchange message based on the public key algorithm determined with the hello messages.
  - If the client has sent a certificate, the client verifies the server certificate and sends a `certificate verify` message indicating the result.

  The client then sends a `finished` message indicating the negotiation part is completed. The client also sends a `change cipher spec` message to generate shared secrets. It should be noted that this is not controlled by the handshake protocol, the change cipher spec protocol manages this part of the operation.
- Step **4**: The server sends a `finished` message indicating the negotiation part is completed. The server then sends the `change cipher spec` message.
- Step **5**: Finally, the session partners separately generate an encryption key, in which they derive the keys to use in the encrypted session that follows from the master key. The Handshake protocol changes the state to the connection state. All data taken from the application layer is transmitted as special messages to the other party.

The SSL Record Protocol transfers application data using the encryption algorithm and keys agreed upon during the handshake phase. As explained above, symmetric encryption algorithms are used, because they provide much better performance than asymmetric algorithms.

SSL considerations

As discussed, security functions such as SSL are needed to send sensitive data safely if you connect your system to an insecure network such as the Internet. On the other hand, using such security functions has performance impacts, including utilizing additional CPU cycles and degrading Web server performance.

Furthermore, SSL does not satisfy every security requirement. While it protects against eavesdropping and alteration of data, it cannot protect the server from an attacker masquerading as a trusted user. For these security concerns, the risk can be minimized by the use of access controls or firewalls.

To maintain SSL security, you have to manage the key carefully, especially when using self-signed certificates, because the whole system environment is affected by the security of the Certificate Authority's key database.

Transport Layer Security Protocol (TLS)

Continued development of the SSL protocol moved into the hands of the Internet Engineering Task Force in 1996. As a result, SSL 3.0 evolved into the proposed standard for Transport Layer Security, RFC 2246.

So, what exactly is new in TLS? It might as readily have been titled SSL 3.1. The protocol syntax and handshake flow remains virtually unchanged. The significant difference is that the hello message for TLS must contain Version 3.1. Once it has been agreed by both client and server that 3.1 is to be used, cipher suite exchanges will use a prefix of TLS_ instead of the SSL 3.0 prefix of SSL_.

Enhancements from SSL V3.0 to TLS V1.0 include:

- Additions to the number of "alert" messages defined in the protocol
- Standardized method of calculating message authentication codes (MAC)
- Simplified CertificateCertify message

Telnet-negotiated sessions

Host On-Demand and Personal Communications Version 5.7 support Telnet-negotiated sessions. Telnet-negotiated session protocol is based on an IETF Internet draft that allows the negotiation of the secure protocol (SSL) prior to establishing the Telnet connection. This draft allows Telnet servers that support SSL V3.0, but not the full TLS RFC (RFC 2246), to negotiate a secure SSL connection.

How does this Internet draft work? It adds a new Interpret As Command (IAC) option and sub-option. The START_TLS option allows the client (WILL START_TLS) or the server (DO START_TLS) to initiate a request for a secure session. Once TLS has been agreed upon, the session immediately drops into negotiation of either SSL or TLS. Negotiation of other Telnet IAC options is suspended until the security negotiation has successfully completed.

If the client and server cannot agree upon the START_TLS option, then the Telnet server can opt to drop into native TLS/SSL security negotiation (identified by CONNTYPE SECURE in the TCP/IP profile data set).

Why add a new IAC option? The foremost advantage is that this option places the control of session security into the TN3270 world (instead of leaving it up to the transport layer). If a Telnet client will not accept a DO START_TLS option, the Telnet server can choose to end the session (CONNTYPE NEGTSECURE in the TCP/IP profile data set).

The other significant advantage of placing encryption negotiation into the TN3270 option data stream is that a single port can be used for encrypted and non-encrypted sessions. Prior to negotiated Telnet, a separate port for secure and non-secure sessions had to be used. Since all TN3270 clients default to port 23, this was not an ideal situation.

A typical negotiated Telnet TLS flow is shown in Figure A-23.

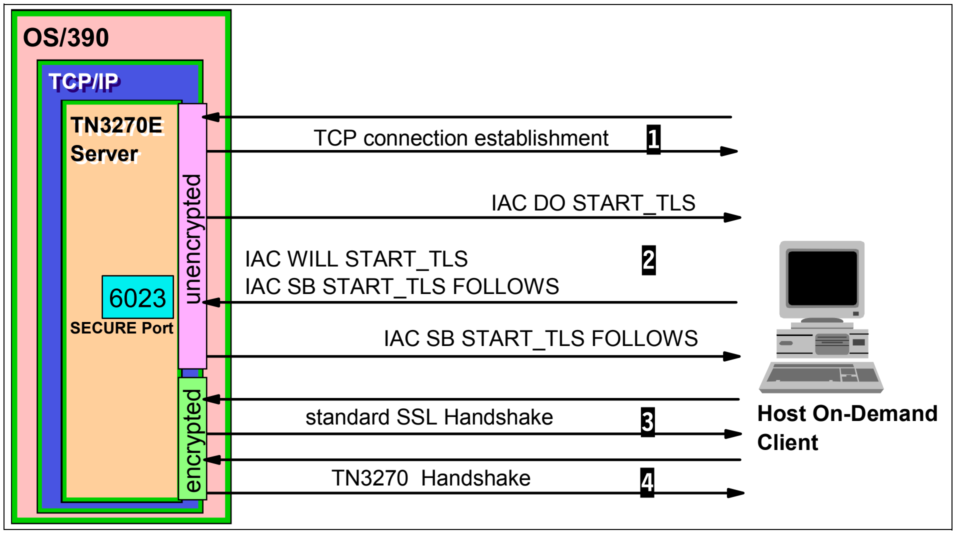


Figure A-23 Telnet-negotiated security session negotiation

Here are the steps:

1. IP connection establishment
2. The Telnet server sends the **IAC DO START_TLS** command to the client to verify if it wants to perform the SSL negotiation.
3. If a positive response is received, then Telnet begins a normal SSL handshake.
4. If no positive response is received, the connection will be dropped.

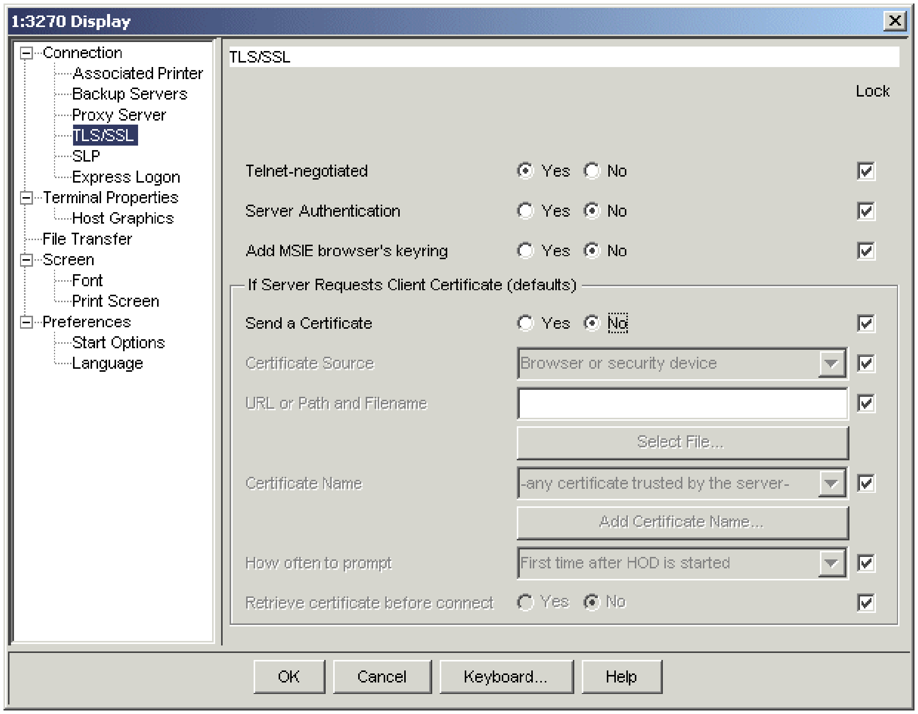
The IAC DO START_TLS Telnet command, sent from the server, activates TLS at the beginning of a Telnet connection. The client can respond to this command by sending the IAC WILL START_TLS command, if the negotiation of a TLS connection is required. With the IAC DONT START_TLS command, the client can refuse the TLS connection negotiation. Sending the IAC SB START_TLS FOLLOWS IAC SE command initiates a TLS negotiation. When this sub-command has been sent and received, the TLS negotiation will begin.

Session configuration

Additional information on session configuration for security can be found at “3270/5250 TLS/SSL selection” on page 291, and 11.4, “Defining a secure Telnet session” on page 427.

In order to implement a Telnet-negotiated session you must first select **Telnet - TLS** as the protocol at the Connection selection. If the Telnet server cannot negotiate a TLS session, **Telnet SSL - only** must be selected.

To activate the Telnet-negotiated radio button, then select the **Yes** radio button for Telnet-negotiated as shown in Figure A-24.



Telnet-negotiated ● Yes ○ No ☑

Server Authentication ○ Yes ● No ☑

Add MSIE browser's keyring ○ Yes ● No ☑

If Server Requests Client Certificate (defaults)

Send a Certificate ○ Yes ● No ☑

Certificate Source: Browser or security device ☑

URL or Path and Filename: ☑

Select File...

Certificate Name: -any certificate trusted by the server- ☑

Add Certificate Name...

How often to prompt: First time after HOD is started ☑

Retrieve certificate before connect ○ Yes ● No ☑

Figure A-24 Enable Telnet-negotiated security

If one of the secure protocols was selected and Telnet-negotiated is **Yes**, then the Telnet connection will be started normally without SSL or TLS. However, the 3270 session will not start until the SSL negotiation completes successfully. If the server `WONT STARTTLS`, then the session will not start, and an error message will be issued stating: `Security was requested, but the server does not support security`.

If **Telnet** was selected as the protocol and the server requests to start the session using Telnet-negotiated security, Host On-Demand will not start the session and an error message will be displayed on the status bar stating: `The server requested security, but Security is not enabled.`

Selecting **Telnet-negotiated** determines if the TLS/SSL negotiation between the client and the server is done on the Telnet connection, or on a TLS/SSL connection prior to the Telnet negotiations. The other options are valid regardless of whether the Telnet-negotiation is enabled. If **Yes** is selected for Telnet-negotiated, then the Telnet protocol will be used to negotiate the SSL security after the Telnet connection is established. This support is only applicable with a Telnet server that supports Telnet-negotiated security. Communications Server for OS/390 V2R10, or above, is the only IBM Telnet Server at this time that supports this function. If **No** is selected for Telnet-negotiated, the traditional TLS/SSL negotiations will be done on a TLS or SSL connection with the server, and subsequently the Telnet negotiations with the server will be done. The default is **No**.

The Communications Server for OS/390 documentation refers to this feature as “negotiable SSL.”

B

Service Location Protocol

Service Location Protocol (SLP) specifies a method to provide dynamic directory services specifically for finding servers by attributes rather than by name or address. In so doing, SLP provides a standard method of allocating service requests among a set of servers with some level of workload balancing. SLP uses multicast services to locate SLP components and Unicast services to communicate between components.

Overview

As businesses expand the scope of their network resources by connecting corporate LANs and WANs with TCP/IP-based intranets, TN3270E servers play an increasingly important role in providing mainframe host connectivity to TCP/IP-based clients. Service Location Protocol (SLP) allows corporate in-house “intranet” environments using Internet standards, in conjunction with TN3270E servers and emulators to provide fast, reliable and cost-effective load-balanced host sessions for end users.

For information on configuring SLP support in HOD clients, see“3270/5250 Connection selection” on page 280, and “3270 Associated Printer selection” on page 285.

Service Location Protocol

Service Location Protocol is a new Internet Engineering Task Force (IETF) proposed standard protocol that was designed to simplify the discovery and use of network resources. In a corporate intranet, users need to access services and resources on the network. Often, it is not clear to the users what useful services are available to them. These resources could include TN3270E servers, Web servers, printers, fax machines, file systems, databases, and any other future services that might become available. IBM Communications Server for AIX, Version 6 supports SLP in conjunction with TN3270E servers and clients such as Host On-Demand SLP clients.

SLP is defined in Request for Comments (RFC) 2165. It is a service-discovery method for TCP/IP-based communications, providing a simple and lightweight protocol for automatic advertisement and maintenance of intranet services and minimizing the use of broadcast and multicast in the network. SLP uses multicast, which targets a group of nodes, unlike broadcast, which targets all nodes. The benefit of multicast is that it sends one packet that all members of the group receive, but that only the intended recipients read. A multicast packet is not isolated to a local segment; routes can forward it to whatever subnets are attached.

Without SLP, users find services by using the name of a network host (a human-readable text string) that is an alias for a network address. Service Location Protocol eliminates the need for a user to know the name of a network host supporting a service. Service Location Protocol allows the user to bind a service description to the network address of the service.

SLP provides a dynamic configuration mechanism for applications in local area networks. It is not a global resolution system for the entire Internet; rather it is intended to serve enterprise networks with shared services. Applications are modeled as clients that need to find servers attached to the enterprise network at a possibly distant location. For cases where there are many different clients and services available, the protocol is adapted to make use of nearby directory agents that offer a centralized repository for advertised services.

SLP terminology

SLP defines specialized components called *agents* that perform tasks and support services as shown in Figure B-1:

- **User Agent (UA)**

  Supports service query functions. It acquires/requests service information for user applications. The user agent retrieves service information from the service agent or directory agents. A Host On-Demand client is an example of a user agent.

- **Service Agent (SA)**

  Service registration and service advertisement. Communications Server V6 for AIX is an example of a Telnet service agent.

- **Directory Agent (DA)**

  Collects service information from service agents to provide a repository of service information in order to centralize it for efficient access by user agents. There can only be one DA present per given host.

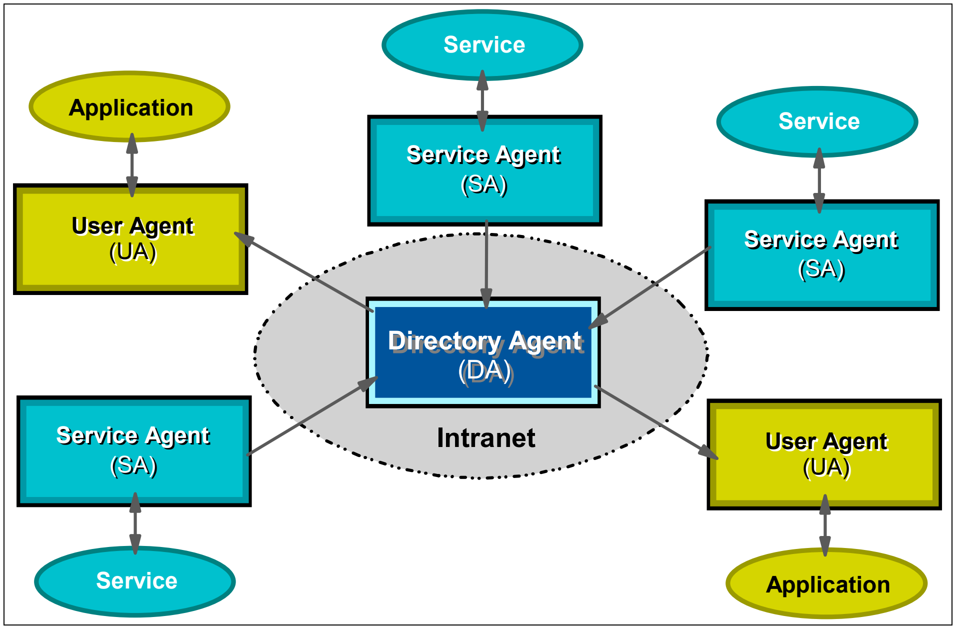


Figure B-1   Service Location Protocol agents

IBM Communications Server for AIX, Version 6 can perform the role of a service agent advertising TN3270 server services. Host-On-Demand, Personal Communications, and other SLP-enabled TN3270 clients perform the role of user agents.

Services are described by the configuration of attributes associated with a type of service. For instance, a CS/AIX configuration providing TN3270 Telnet gateway access to an SNA network through the TN3270 protocol would define a service called TN3270 with a set of associated attributes. A TN3270 client (user agent) would select the appropriate TN3270 attributes group that it needs in a service request message to a directory agent, or directly to service agents, and await a reply. In small installations, there may be no directory agents, and the request message from the TN3270 client would be sent (multicast) directly to the service agents.

A user agent can select an appropriate service by specifying the attributes that it needs in a service request message. When service replies are returned (assuming multiple service agents can satisfy the request), they contain a Uniform Resource Locator (URL) pointing to the service desired, and other information such as the server load needed by the user agent.

The Host On-Demand client is the user agent; Communications Server for Windows NT and Windows 2000 or Communications Server for AIX is the service agent.

The following is additional terminology used when discussing SLP:

- **Service**

  The service is a process or system (such as TN3270 server, Web server, and so on) providing a function or service to the network. The service itself is accessed using a communication mechanism external to the Service Location Protocol.

- **Service Information**

  A collection of attributes and configuration information associated with a single service. The service agents advertise service information for a collection of service instances.

- **Site Network**

  All the hosts accessible within the agent's multicast radius, which defaults to a value appropriate for reaching all hosts within a site. If the site does not support multicast, the agent's site network is restricted to a single subnet.

- **Scope**

  A collection of services that make up a logical group.

SLP can reduce overall network traffic by using scopes to manage client service requests. A scope is essentially a grouping method to organize servers into named groups. Scope values are defined by a network administrator, and may represent departments, regions, or organizations. If desired, different scopes can be assigned for different services provided on the server.

Load balancing

Load balancing using SLP dynamically balances user agent sessions by distributing them to the service agent (which supports the desired service) with the smallest load. TN3270 clients that support load balancing have the ability to query participating SLP TN3270E servers and connect to the least loaded service agent (for example, a CS/AIX TN3270 server gateway).

The SLP load balancing weight factor gives the administrator the ability to modify or weight the load balancing measurement for each server. The factor can be different for each server. The measurement can take into account numbers of active sessions, memory constraints and CPU constraints on each server. The weight factor gives the administrator an element of control in this calculation. The weighting factor is useful because:

- In some cases, there are other factors that may have an effect on server load that are not taken into account by the server load algorithm, for example, if the server is not dedicated to SNA gateway traffic only.
- If the server providing TN3270 services must coexist in a network with other TN server implementations using SLP for load balancing, the load factor can be adjusted to compensate for differences between server machines.

The weight factor allows the administrator to bias the load measurement on that server either away from or towards selecting the server. The factor can be turned on or off as well, causing it to be ignored in load calculations.

As shown in Figure B-2, when a TN3270 client requests a session to the host, those servers that support TN3270 services respond with their current load. The least loaded TN3270 server will be chosen by the client to make connection to the host.

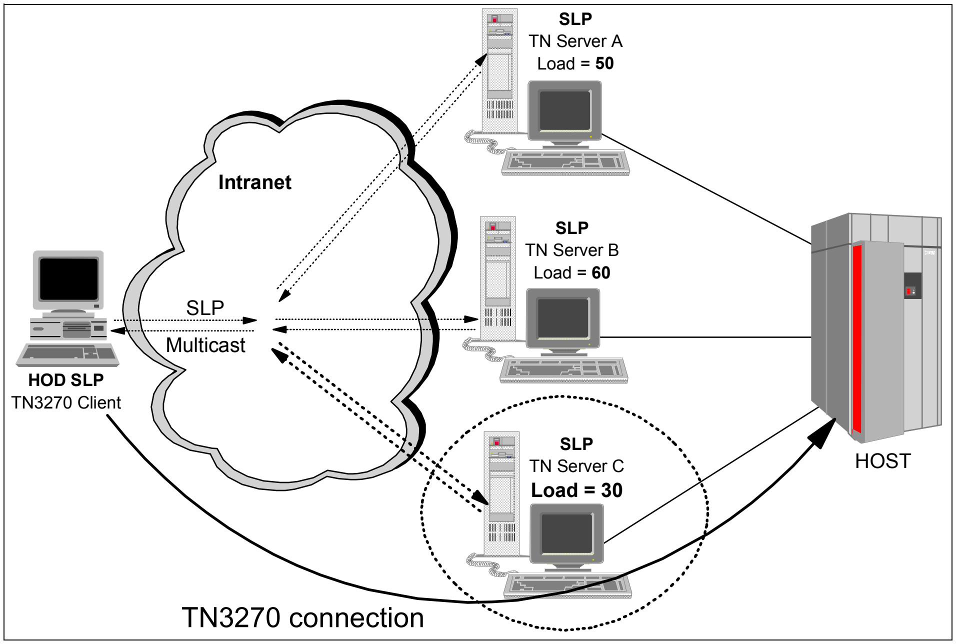


Figure B-2 Service Location Protocol load balancing with Host On-Demand client

Note that both the TN3270 client and TN3270 server must support SLP and the load balancing process.

Communications Server for Windows NT and Windows 2000 or Communications Server for AIX provide information about the server load, using SLP, by calculating the percentage of available resources. For LUA sessions, such as 3270 sessions, the load percentage is the number of active application connections divided by the total number of LUs available.

The Host On-Demand client gets the load percentage through SLP, determines which server is the least loaded, and attempts a connection to that server.

In Figure B-2, the client has three servers available for the client connection. The Host On-Demand client will attempt to connect to TN Server C because, according to the load values returned, it is the least loaded of the three. If the connection is successful, the load of Server C will increase. If this increase means that Server C is no longer the least loaded, the next SLP client will realize that and connect to a different server.

Scope

SLP can reduce overall network traffic by using scopes to manage client service requests. A scope is essentially a grouping method used to organize servers into named groups or pools. This is ideal for large networks with a number of gateways or servers.

Scope can be looked at in two different ways:

- Scope is a *mechanism* in Service Location Protocol that provides the capability to organize a site network along administrative lines. A set of services can be assigned to a given department of an organization, to a certain geographical area, or for a certain purpose.
- Scope is a *parameter* used to control and manage access by workstations (user agents) to TN3270 servers (service agents) in a network.

Scope values are defined by a network administrator, and may represent departments, regions, or organizations. If desired, different scopes can be assigned for different services provided on the server.

For an example, see Figure B-3.

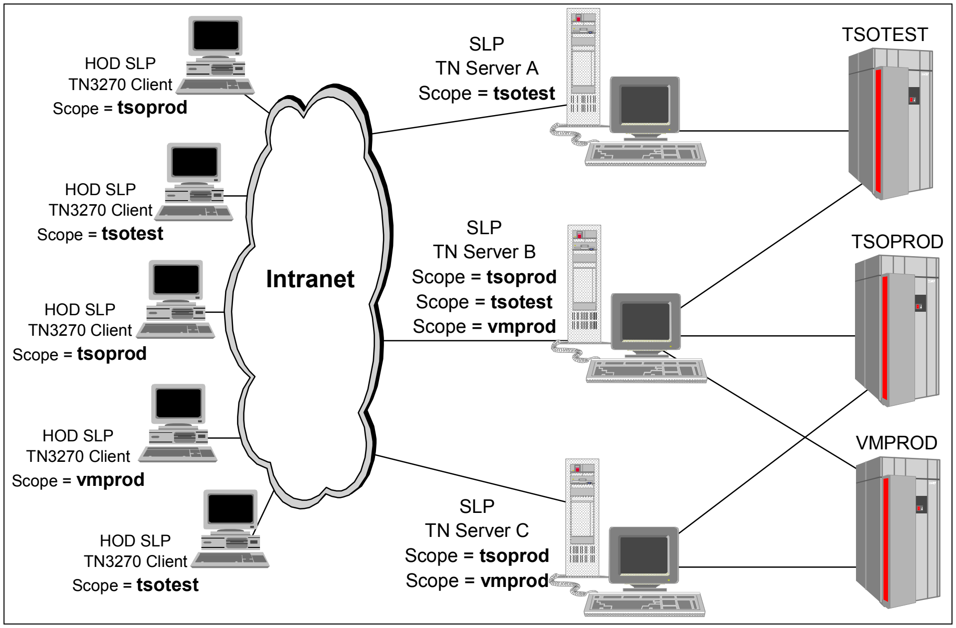


Figure B-3 Service Location Protocol scope example

In the example network shown in Figure B-3, CS/AIX Server A has only one scope defined (TSOTEST) and is attached to only one host. However, Server B is attached to three different hosts and advertises three different scopes (TSOPROD, TSOTEST and VMPROD). Server C advertises scopes TSOPROD and VMPROD.

In this configuration, HOD clients using scope TSOPROD will balance between CS/AIX Servers B and C, while HOD clients using other scopes will balance between the servers that can provide that particular class of LU. In addition, specification of scope on the client platform supports the use of wildcards. For example, a client that specifies a scope of TSO* can select between servers that advertise scopes of TSOTEST and TSOPROD.

Warm standby

Warm standby is available for TN3270 and TN5250 sessions through SLP. If the current connection fails, and if the client's Auto-Reconnect option is set to `Yes`, the client queries the servers again and connects to the least loaded.

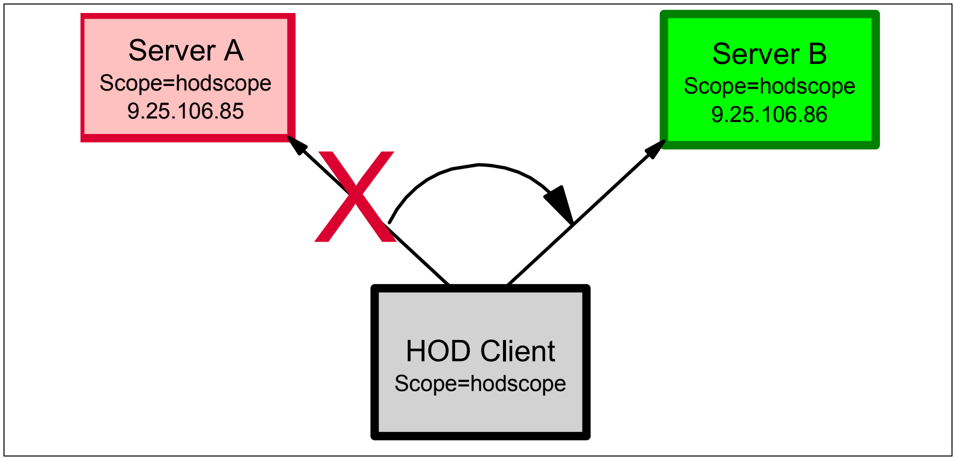


Figure B-4 Host On-Demand warm standby with SLP

SLP review

The basic operation in Service Location Protocol is that a client attempts to discover the location of a service. In smaller installations, each service will be configured to respond individually to each client. In larger installations, services will register their services with one or more directory agents, and clients will contact the directory agent to fulfill requests for Service Location information.

A large network can be divided and categorized by the use of scopes, so that information about a TN server is advertised only to TN3270 clients and directory agents that have the same scope as the TN server. This allows you to control the range of service searches.

The following describes the operations a user agent would employ to find services on the site's network. The user agent needs no configuration to begin network interaction. The user agent can acquire information to construct predicates that describe the services that match the user's needs. The user agent may build on the information received in earlier network requests to find the service agents advertising service information.

A user agent will operate two ways:

- If the user agent has already obtained the location of a directory agent, the user agent will Unicast a request to it in order to resolve a particular request. The directory agent will Unicast a reply to the user agent. The user agent will retry a request to a directory agent until it gets a reply, so if the directory agent cannot service the request it must return an response with zero values, possibly with an error code set.

- If the user agent does not have knowledge of a directory agent or if there are no directory agents available on the site network, a second mode of discovery may be used. The user agent multicasts a request to the service-specific multicast address, to which the service it wishes to locate will respond. All the service agents that are listening to this multicast address will respond, provided they can satisfy the user agent's request.

A directory agent acts on behalf of many service agents. It acquires information from them and acts as a single point of contact to supply that information to user agents.

C

An example of MacroIOProvider

```
//*****************************************************************************
  // MacroIOProvider implementation...
  //
  // For this demo, the IO Provider will just maintain the macros in memory.
  // Macros will be alive only for the duration of the applet. Use this code
  // as a base to write your macros out to your server or local disk. Please
  // pay attention to what file privilages you have when doing so.
  //
  // MacroManager provides a default MacroIOProvider that saves the macros to
  // wherever the class was loaded from. This works well if the bean is used
  // in an application, or if it used in an applet with Navigator 4.x
  // and Internet Explorer 4.x, which should have the right privilages enabled.
  //*****************************************************************************

  /*****************************************************************************
  * Saves a macro to persistent storage.  The macro is supplied in the form of
  * a property which contains the macro name, description, and source code
text.
  *
  * @param prop A properties object representing the macro to be saved.
  * @see #getMacro(String)
  */
  public void putMacro(Properties p)
  {
```

```
  Properties props = null;
  String nameToSave = (String)p.get(Macro.NAME);

  // Search through list and remove if already exists
  for (int i = 0; i < macroList.size(); i++) {
      props = (Properties)macroList.elementAt(i);
      if (((String)props.get(Macro.NAME)).equals(nameToSave)) {
          macroList.removeElement(props);
          break;
      }
  }

  // Add the element
  macroList.addElement(p);
}

/*****************************************************************************
* Retrieves a macro from persistent storage.  The macro name is supplied and
* the macro is returned in the form of a properties object which
* contains the macro name, description, and source code text.
*
* @param name String containing the name of the macro to be retrieved.
* @see #putMacro(Properties)
*/
public Properties getMacro(String name)
{
  Properties retProps = null;

  // Search through list for name and return if there, null by default
  for (int i = 0; i < macroList.size(); i++) {
      retProps = (Properties)macroList.elementAt(i);
      if (((String)retProps.get(Macro.NAME)).equals(name))
          return retProps;
  }

  return null;
}

/*****************************************************************************
* Deletes a macro from persistent storage.
*
* @param name String containing the name of the macro to be deleted.
*/
public void removeMacro(String name)
{
  Properties retProps = null;

  // Search through list and remove the macro
  for (int i = 0; i < macroList.size(); i++) {
      retProps = (Properties)macroList.elementAt(i);
      if (((String)retProps.get(Macro.NAME)).equals(name)) {
          macroList.removeElement(retProps);
          break;
      }
  }
}

/****************************************************************************
* Returns a list of all the macros in persistent storage.  The returned
* Vector should contain a set of Properties object, each of which contains
* (at a minimum) a macro name and description.  The properties objects
* do not need to (but may) contain the macro source code text.  The
* MacroManager will issue a getMacro() call to retrieve the macro source
* text when required.
*
* @see #getMacro(String)
*/
public Vector listMacros()
{
  return macroList;
}
```

D

Web Express Logon

This appendix includes the password encryption tool.

Password encryption tool

Host On-Demand provides a password encryption tool so you can encrypt your passwords for added security. It is a command-line tool that allows you to generate a file that stores the encrypted password, which you must then copy to the appropriate place in the web.xml file. The Host Credential Mapper (HCM) plug-in decrypts the password before using it.

If you create a custom Host Credential plug-in, the plug-in should use the com.ibm.eNetwork.HOD.common.PasswordCipher object to decrypt the password. The CLASS file for this object is included in WAR file. Refer to Custom Credential Mapper Servlet response object for a description of the encrypt and decrypt methods.

Microsoft Windows platforms

Using a DOS prompt, change the current directory to the Host On-Demand's bin directory and type the following command:

```
encrypt <password> [filename]
```

where *<password>* is the password to be encrypted and *[filename]* is the name of the file that you want to use to store the encrypted password. The default filename is password.txt.

UNIX platforms:

Issue the following command:

```
cd your_install_dir
Java -classpath .;your_install_dir\lib\sm.zip \
com.ibm.eNetwork.security.sso.cms.tools.Encrypt <password> [filename]
```

where *your_install_dir* is your Host On-Demand installation directory, *<password>* is the password to be encrypted, and *[filename]* is the name of the file that you want to store the encrypted password. The default filename is password.txt.

E

Additional material

This redbook refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material associated with this redbook is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser to:

```
ftp://www.redbooks.ibm.com/redbooks/SG246182
```

Alternatively, you can go to the IBM Redbooks Web site at:

```
http://www.ibm.com/redbooks
```

Select the **Additional materials** and open the directory that corresponds with the redbook form number, SG24-6182.

Using the Web material

The additional Web material that accompanies this redbook includes two separate, working demonstrations of using the Session Manager API to enhance a host application. One demo is for a Java 1 browser environment while the other is for Java 2. There are two separate ZIP files:

File name	*Description*
JSDemoEJ1.zip	Zipped code samples for a Java 1 environment
JSDemoEJ2.zip	Zipped code samples for a Java 2 environment

Java 1 demo (JSDemoEJ1.zip)

The following files are in the HostOnDemand\HOD directory:

JSAPIDemoJ1.html File created by the Deployment Wizard; the administrator has selected **Java 1** as the client Java type.

JSDemoHelp.html This file opens in the bottom frame when users click the **Demo Help** button; it shows you how to run the demonstration and to learn more about how it works.

JSDemoIEJ1.html The main Web site; it divides the page into three frames, with 36% allocated to the first frame, 64% allocated to the second frame, and 0% allocated to the third frame.

JSNavigation.html This is what displays in the first frame of the main Web site; it contains all the navigation buttons.

JSWelcome.html This file opens in the bottom frame when users click the **Welcome** button; is provides a simple scenario that demonstrates how to store data in the Web page and send it to the Host On-Demand applet.

The following files are in the HostOnDemand\HOD\HODData\JSAPIDemoJ1 directory:

> **Note:** These files contain the session configuration information created by the administrator. Remember that when you create HTML files using the Deployment Wizard, a corresponding subdirectory is created with the same name under \HODData. In this case, the Deployment Wizard file is called JSAPIDemoJ1.html, so the corresponding subdirectory is also called \JSAPIDemoJ1.

cfg0.cf Contains configuration information for one of the three sessions defined by the administrator

cfg1.cf Contains configuration information for one of the three sessions defined by the administrator

cfg2.cf Contains configuration information for one of the three sessions defined by the administrator

params.txt Contains Host On-Demand configuration parameters

policy.obj Contains information about the Disabled Functions

preloads.obj Contains information about the objects to preload as defined on the Preload Options window

udparams.txt User-defined HTML parameters

wInfo.txt Contains the responses to each window in the Deployment Wizard; used only by the Deployment Wizard

In addition, the JSDemoEJ1.zip file contains various .gif files that make up the images included in the demonstration files.

Java 2 demo (JSDemoEJ2.zip)

The following files are in the HostOnDemand\HOD directory:

JSAPIDemoJ2.html File created by the Deployment Wizard; the administrator has selected **Java 2** as the client Java type.

JSDemoHelp.html This file opens in the bottom frame when users click the **Demo Help** button; it shows you how to run the demonstration and to learn more about how it works.

JSDemoIEJ2.html The main Web site; it divides the page into three frames, with 36% allocated to the first frame, 64% allocated to the second frame, and 0% allocated to the third frame.

JSNavigation.html This is what displays in the first frame of the main Web site; it contains all the navigation buttons.

JSWelcome.html This file opens in the bottom frame when users click the **Welcome** button; is provides a simple scenario that demonstrates how to store data in the Web page and send it to the Host On-Demand applet.

z_JSAPIDemoJ2.html This file is generated for Java2 or Auto selection in Deployment Wizard; it is the final page that is displayed after the Java2 and Autodetection is done.

The following files are in the HostOnDemand\HOD\HODData\JSAPIDemoJ2 directory:

> **Note:** These files contain the session configuration information created by the administrator. Remember that when you create HTML files using the Deployment Wizard, a corresponding subdirectory is created with the same name under \HODData. In this case, the Deployment Wizard file is called JSAPIDemoJ2.html, so the corresponding subdirectory is also called \JSAPIDemoJ2.

cfg0.cf	Contains configuration information for one of the three sessions defined by the administrator
cfg1.cf	Contains configuration information for one of the three sessions defined by the administrator
cfg2.cf	Contains configuration information for one of the three sessions defined by the administrator
params.txt	Contains Host On-Demand configuration parameters
policy.obj	Contains information about the Disabled Functions
preloads.obj	Contains information about the objects to preload as defined on the Preload Options window
udparams.txt	User-defined HTML parameters
wlnfo.txt	Contains the responses to each window in the Deployment Wizard; used only by the Deployment Wizard

In addition, the JSDemoEJ2.zip file contains various .gif files that make up the images included in the demonstration files.

System requirements for downloading the Web material

The following system configuration is recommended:

Hard disk space:	250 KB minimum
Operating system:	Windows 2000 with Internet Explorer

How to use the Web material

You can extract the contents of the demonstration zip files (`JSDemoEJ1.zip` and `JSDemoEJ21.zip`)either directly into the Host On-Demand publish directory, or you can extract them into a separate directory and manually copy the files into the publish directory. The files must be in the publish directory in order for the demonstration to work properly.

The Java 1 and Java 2 demonstrations can co-exist in the same directory. Note that the two demonstrations have several files in common, so if you unzip both demonstrations into the same directory, you will be asked if you want to overwrite these files. You can accept the overwrite.

Abbreviations and acronyms

ACL	access control list
ACPI	Advanced Configuration and Power Interface
ADO	ActiveX Data Object
AES	Advanced Encryption Standard
AFP	Advanced Function Printer
AFS	Andrew File System
AFTP	APPC File Transfer Protocol
AH	Authentication Header
AIX	Advanced Interactive eXecutive
ANSI	American National Standards Institute
AOR	application owning region
APAR	authorized program analysis report
API	application programming interface
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking®
ARP	Address Resolution Protocol
AS/IMS	Application Support/IMS
asate	application service at the edge
ASCII	American National Standard Code for Information Interchange
ASID	address space ID
ATI	automatic transaction initiation
ATM	Asynchronous Transfer Mode
ATRN	ASCII Transparency
AWT	Abstract Windowing Toolkit
BF	BestFit
BIDI	bidirectional
BIND	Berkeley Internet Name Domain
BLT	Basic License Tool
BMP	Batch Message Program, Bean Managed Persistence
BMS	Basic Mapping Support
CA	Certificate Authority
CAB	cabinet
CAE	Client Application Enabler
CAPI	cryptographic application programming interface
CARP	Cache Array Routing Protocol
CB	Component Broker
CBPDO	Custom Built Product Delivery Offering
CBR	Content Based Routing
CCF	Common Connector Framework
CCI	Common Client Interface
CD	compact disc
CDC	Content Distribution Client
CDF	Content Distribution Facility, Content Distribution Framework
CDMF	Commercial Data Masking Facility
CDN	Content Distribution Network
CDS	Content Distribution System
CECI	Command Level Interpreter Transaction
CGI	Common Gateway Interface
CICS	Customer Information Control System
CLI	Call Level Interface
CMS	Conversational Monitor System
CMS	Credential Mapper Servlet
CN	common name
COMMAREA	communications area
CORBA	Common Object Request Broker Architecture
CPI	characters per inch
CPU	central processing unit

CR	carriage return
CRLF	carriage return, line feed
CS	Communications Server
CS/AIX	Communications Server/AIX
CSD	corrective service delivery, corrective service distribution, corrective service diskette
CSI	Consolidated Software Inventory
CSS	Cascading Style Sheet
CTG	CICS Transaction Gateway
CWS	CICS Web support
DA	directory agent
DASD	Direct Access Storage Device
DB2LSX	DB2 LotusScript Extension
DBCS	double byte character set
DCAR	Digital Certificate Access Requestor
DCAS	Digital Certificate Access Server
DCE	Distributed Computing Environment
DDCS	Data Definition Control Support
DDE	dynamic data exchange
DDF	Distributed Data Facility
DDNS	Dynamic Domain Name System
DEC	Digital Equipment Corporation
DECS	Domino Enterprise Connection Services
DES	Data Encryption Standard
DFT	distributed function terminal
DH	Diffie-Hellman
DHCP	dynamic host configuration protocol
DIT	Directory Information Tree
DLUR	dependent LU requestor
DMT	Directory management tool
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DOM	Document Object Model
DPI®	dots per inch
DPL	Distributed Program Link
DRDA®	Distributed Relational Database Architecture
DSCP	Differentiated Services Control Point
DTD	document type definition
DTP	Distributed Transaction Processing
EAB	Enterprise Access Builder
EAI	Enterprise Application Integration
EAR	Enterprise Archive file
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECA	External Cache Adapter
ECI	External Call Interface
ECLPS	Emulator Class Library Presentation Services
EE	Enterprise Extender
EHLLAPI	enhanced high level language application programming interface
EIS	Enterprise Information Systems
EJB	Enterprise JavaBeans
EJS	Enterprise Java Services
ELF	Express Logon Feature
ELP	enhanced local preferences
ENPTUI	Enhanced Non-Programmable Terminal User Interface
EPI	External Presentation Interface
ESA	Enterprise Systems Architecture
ESC/P	Epson standard code for printers
ESI	Edge side includes, External Security Interface
ESP	Encapsulating Security Payload
EXCI	External CICS Interface
FCRA	Fast Cache Response Accelerator
FDDI	Fiber Distributed Data Interface
FEPI	Front End Programming Interface

FIPS	federal information processing standard
FMID	function modification identifier
FTP	file transfer protocol
GC	garbage collector
GDDM®	Graphical Data Display Manager
GDI	graphical device interface
GEM	Global Enterprise Manager
GID	Group Identification Number
GIF	Graphics Interchange Format
GRE	Generic Routing Encapsulation
GSK	Global Security Toolkit
GUI	Graphical User Interface
GWAPI	Go Webserver API
HAB	Host Access Beans
HABJ	Host Access Beans for Java
HACL	Host Access Class Library
HACLJ	Host Access Class Library for Java
HACMP	High Availability Cluster Multiprocessing
HACP	Host Access Client Package
HFS	Hierarchical File System
HLLAPI	high level language application programming interface
HMAC	Hashed Message Authentication Code
HOD	Host On-Demand
HPR	high performance routing
HPT	host print transform
HP-UX	Hewlett-Packard UNIX
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAC	interpret as command
IBM	International Business Machines Corporation
ICAPI	Internet Connection Application Programming Interface
ICP	Internet Caching Protocol
ICSF	integrated cryptographic service facility
ICU	International Component for Unicode
IDE	Integrated Development Environment
IDEA	International Data Encryption Algorithm
IDL	Interface Definition Language
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHS	IBM HTTP Server
IIOP	Internet Inter-ORB Protocol
IKE	Internet Key Exchange
IMAP	Internet Mail Access Protocol
IME	Input Method Editor
IMS	Information Management System
IMS/ESA®	IMS/Enterprise Systems Architecture
IP	Internet Protocol
IPL	initial program load
IPSec	IP Security Architecture
ISAKMP	Internet Security Association and Key Management Protocol
ISC	Inter-System Communication
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISS	Interactive Session Support
IT	Information Technology
ITOC	IMS TCP/IP OTMA Connection
ITSO	International Technical Support Organization
IWT	IMS Web Templates
J2EE	Java 2 Enterprise Edition
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition

JAR	Java archive
JCA	Java Connector Architecture
JCL	job control language
JDBC	Java Database Connectivity
JDK	Java developer kit
JIT	just in time
JITOC	Java IMS TCP/IP OTMA Connection Connector
JNDI	Java Naming and Directory Interface
JNI	Java Native Interface
JNLP	Java Network Launch Protocol
JPEG	Joint Photographic Experts Group
JRE	Java runtime environment
JSP	JavaServer Pages
JTA	Java Transaction API
JVM	Java Virtual Machine
L2TP	Layer 2 Tunnel Protocol
LAN	local area network
LC LSX	Lotus Connector LotusScript Extension
LDAP	Lightweight Directory Access Protocol
LDIF	Lightweight Directory Interface File
LED	light emitting diode
LEI	Lotus Enterprise Integrator®
LLC2	link level control 2
LPAR	Logical partition mode
LPI	lines per inch
LSX	LotusScript Extension
LTPA	Lightweight third party authentication
LU	logical unit
LUM	license use manager
MAC	Media Access Control, Message Authentication Code
Mbps	megabits per second
MBps	megabytes per second
MCDS	Master Content Distribution Server
MIB	management information base
MIME	Multipurpose Internet Mail Extensions
MPA	multi-protocol adapter
MPP	Message Processing Program
MQ	Message and Queueing
MQEI	MQSeries® Enterprise Integrator
MQI	Message and Queueing Interface
MQLSX	MQSeries Link LotusScript Extension
MQM	Message Queue Manager
MSI	Microsoft Installer
MSIE	Microsoft Internet Explorer
MVS	Multiple Virtual Storage
NAP	network access points
NAT	Network Address Translation
NCSA	National Center for Supercomputing Applications
ND	Network Dispatcher
NDIS	network driver interface specification
NFA	Non-forwarding address
NFS	network file system
NIC	Network Interface Card
NIST	National Institute for Standards and Technology
NLS	National Language Support
NNTP	NetNews transfer protocol
NPT	non-programmable terminal
NSA	National Security Agency
ODBC	Open Database Connectivity
ODG	object dependency graph
ODS	object data store
OHIO	Open Host Interface Objects
OIA	operator information area
OLE	object linking and embedding
OLTP	On-Line Transaction Processing
OMG	Object Management Group
ORB	Object Request Broker

OS/2	Operating System/2®
OSA	Open Systems Adapter
OSE	open servlet engine
OSF	Open Software Foundation
OTMA	Open Transaction Manager Access
PAC	proxy automatic configuration
PCI	Peripheral Component Interconnect
PCL	printer control language
PCOMM	IBM Personal Communications
PD	problem determination
PDF	printer definition file
PDS	partitioned data set
PDT	printer definition table
PGP	Pretty Good Privacy
PGP	Pretty Good Privacy
PICS	Platform for Internet Content Selection
PID	product ID
PIN	personal identification number
PKCS	Public Key Cryptographic Standard
PKDS	Public Key Data Set
PKI	Public Key Infrastructure
POP	points of presence, Protected object policy
POP3	Post Office Protocol 3
PPDS	personal printer definition stream
PPP	Point-to-Point Protocol
PRC	People’s Republic of China
PSP	Preventive Service Planning
PTF	Program Temporary Fix
PWS	programmable workstation
RACF	Resource Access Control Facility
RCA	Remote Cache Access
RDBMS	Relational Database Management System
REXX	Restructured Extended eXecutor Language
RFC	Request for Comment
RGB	red, green, blue
RIO	Remote Integration Object
RMI	remote method invocation
ROC	Republic of China
RPC	Remote Procedure Call
RSA	Rivest, Shamir, and Adleman
RSACI	Recreational Software Advisory Council on the Internet
RTSP	Real Time Streaming Protocol
SA	Security Association
SAP	service access point
SAX	Simple API for XML
SBCS	single byte character set
SCCI	Screen Customizer Component Interface
SCS	SNA character string
SDA	Server Directed Affinity
SDK	Software Development Kit
SDLC	synchronous data link control
SET	Secure Electronic Transactions
SGML	Standard Generalized Markup Language
SHA	secure hash algorithm
SHS	Secure Hash Standard
SLA	Service Level Agreement
SLP	Service Location Protocol
SMA	Server Monitor Agent
SMF	System Measurement Facility
SMP/E	System Modification Program/Extended
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SPARC	Scalable processor architecture

SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEC	Tivoli Enterprise™ Console
TIF	Tagged Image Format
TLS	Transport Layer Security
TM	Transaction Manager, Trigger Monitor
TMR	Tivoli Management Region
TN	Telnet
TOS	Type Of Service
TQoS	Transactional Quality of Service
TSO	Time Sharing Option
TTY	teletypewriter
UA	unnumbered acknowledgement, User Agent
UDC	user-defined characters
UDP	User Datagram Protocol
UID	User Identification Number
URI	Universal Resource Identifier
URL	Universal Resource Locator, Uniform Resource Locator
USB	universal serial bus
USS	Unformatted System Services
USSMSG10	Unformatted Systems Services, message number 10
VB	Visual Basic
VM	virtual machine
VM/CMS	virtual machine/conversational monitor system
VPN	virtual private network
VT	virtual terminal
VTAM	Virtual Telecommunications Access Method
W3C	World Wide Web Consortium
WAN	Wide Area Network
WAND	Wide Area Network Dispatcher
WAP	Wireless Application Protocol
WAR	Web module Archive
WAS	WebSphere Application Server
WAS AE	WebSphere Application Server Advanced Edition
WAS AEs	WebSphere Application Server Advanced Single Server Edition
WCDP	Web Content Distribution Protocol
WCPP	Web Content Publishing Protocol
WLM	workload manager
WML	Wireless Markup Language
WPAD	Web Proxy Auto Discovery
WSAD-IE	WebSphere Studio Application Developer-Integration Edition
WSAM	Web Start Application Manager
WSES	WebSphere Edge Server
WTE	Web Traffic Express
WWW	World Wide Web
XCF	Cross-System Coupling Facility
XLGW	XML Legacy Gateway
XML	eXtensible Markup Language
XSL	eXtensible Style Language

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see "How to get IBM Redbooks" on page 1085:

- *IBM Host Access Client Package Update (HACP V3)*, SG24-6182-01
- *IBM Host Integration in a Secure Network: A Practical Approach*, SG24-5988
- *Programming with the Host Access APIs,* SG24-5856
- *Personal Communications Version 4.3 for Windows 95,98 and NT,* SG24-4689
- *Java 2 Network Security* by M. Pistoia et al., June 1999, IBM Form Number: SG24-2109-01, ISBN: 0-130-15592-6
- *Communication Server for z/OS V1R2 TCP/IP Implementation Guide Volume 1: Base and TN3270 Configuration,* SG24-5227
- *Communication Server for z/OS V1R2 TCP/IP Implementation Guide Volume 7: Security,* SG24-6840
- *AS/400 HTTP Server Performance and Capacity Planning,* SG24-5645
- *Understanding LDAP,* SG24-4986
- *LDAP Implementation Cookbook*, SG24-5110
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*, SG24-6163
- *Deploying a Public Key Infrastructure*, SG24-5512
- *IBM WebSphere V4.0 Advanced Edition Handbook*, SG24-6176
- *TCP/IP Tutorial and Technical Overview*, GG24-3376
- *A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions,* SG24-5201
- *Secure e-business in TCP/IP Networks on OS/390 and z/OS*, SG24-5383

Other resources

These publications are also relevant as further information sources:

- *IBM WebSphere HOD V8 Planning, Installing and Configuring Host On-Demand*, SC31-6301
- *IBM WebSphere Host On-Demand V8.0 Host Printing Reference,* SC31-6353
- *IBM WebSphere Host Access Toolkit V8.0 Getting Started,* SC31-6354
- *IBM WebSphere Host On-Demand V8.0 Session Manager API Reference,* SC31-6355
- *IBM WebSphere Host On-Demand V8.0 Web Express Logon Reference,* SC31-6377
- *IBM WebSphere Host On-Demand V8.0 Host On-Demand Macro Programming Guide,* SC31-6378
- *IBM Programmable Host On-Demand Reference,* SC31-6380
- *Program Directory for IBM WebSphere Host On-Demand V8.0 for OS/390 and z/OS,* GI10-3276
- Host On-Demand online documentation:
  - *Planning, Installing and Configuring Host On-Demand*
  - *Host Printing Reference*
  - *Macro Programming Guide*
  - *Session Manager API Reference*
  - *Programmable Host On-Demand Reference*
  - *Toolkit Getting Started*
  - *Host Access Beans for Java Reference*
  - *Host Access Class Library Reference*
  - *J2EE Connector Reference*
  - *ReadMe*
- *Personal Communications for Windows V5.7,* GC31-8694
- *Personal Communications for Windows V5.7 Quick Beginnings*, SC31-8679
- *Personal Communications for Windows V5.7 Configuration File Reference*, SC31-8655
- *Personal Communications for Windows V5.7 Emulator Programming*, SC31-8478
- *Personal Communications for Windows V5.7 Client/Server Communications Programming*, SC31-8479
- *Personal Communications for Windows V5.7 System Management Programming*, SC31-8480

- *Personal Communications for Windows V5.7 CM Mouse Support User’s Guide and Reference*
- *Personal Communications for Windows V5.7 Administrator’s Guide and Reference*, SC31-8840
- *Personal Communications for Windows V5.7 Host Access Class Library*, SC31-8685
- Personal Communications online documentation:
  - *Quick Beginnings*
  - *CD-ROM Guide to Installation*
  - *Administrator Guide and Reference*
  - *Host Access Class Library*
  - *Client/Server Communications Programming*
  - *Emulator Programming*
- *z/OS HTTP Server Planning, Installing and Using,* SC34-4826
- *SMP/E V3R1.0 for z/OS and OS/390: User's Guide*, SA22-7773
- *SMP/E V3R1.0 for z/OS and OS/390: Reference*, SA22-7772
- *z/OS V1R1.0 MVS Initialization and Tuning Reference*, SA22-7592
- *OS/390 V2R10 IBM Communications Server for IP Configuration Reference,* SC31-8726
- *z/OS V1R2 IBM Communications Server for IP Configuration Reference,* SC31-8776
- *OS/390 SecureWay Security Server LDAP Client Application Development Guide and Reference*, SC24-5878
- *OS/390 SecureWay Security Server LDAP Server Administration and Usage Guide*, SC24-5861
- *z/OS SecureWay Security Server LDAP Server Administration and Usage Guide*, SC24-5923
- *z/OS V1R2 Communications Server: IP Migration*, GC31-8773
- *OS/390 V2R10.0 IBM Communications Server IP Migration Guide,* SC31-8512
- *OS/390 SMP/E User’s Guide*, SC28-1740
- *OS/390 SMP/E Reference*, SC28-1806
- *MVS Initialization and Tuning Reference*, SA22-7592
- *DEC VT220 Programmer Reference Manual*
- *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design,* by Electronic Frontier Foundation, John Gilmore (Editor), 1988

- *The Oakley Key Determination Protocol*, by H. Orman; RFC 2412, November 1998
- *SKEME: A Versatile Secure Key Exchange Mechanism for the Internet*, by H. Krawczyk; IEEE Proceedings, 1996
- *Java Security: 2nd Edition* by Scott Oaks, May 2001, O'Reilly & Associates, Inc. ISBN: 0-596-00157-6

Referenced Web sites

These Web sites are also relevant as further information sources:

- Host On-Demand Internet home page

  http://www.ibm.com/software/webservers/hostondemand

- IBM Host On-Demand InfoCenter and Tutorials

  http://www.ibm.com/software/webservers/hostondemand/library/v8infocenter/hod/en/help/2tabcontents.html

- Host On-Demand downloads

  http://www14.software.ibm.com/webapp/download/product.jsp?s=p&id=RSHY-4L8MH9

- IBM EHLLAPI Bridge support for Host On-Demand

  http://www14.software.ibm.com/webapp/download/preconfig.jsp?id=2002-12-22+21%3A26%3A59.398264R&cat=&fam=&s=p&S_TACT=&S_CMP=

- IBM Express Logon whitepaper (Certificate Express Logon)

  ftp://ftp.software.ibm.com/software/network/library/whitepapers/elf.pdf
  http://www.ibm.com/software/network/library/whitepapers/elf.html

- IBM Express Logon whitepaper (Web Express Logon)

  http://www.ibm.com/software/network/library/whitepapers/wel.pdf

- IBM WebSphere Host On-Demand Support

  http://www.ibm.com/software/webservers/hostondemand/support.html

- Host On-Demand documentation library

  http://www.ibm.com/software/webservers/hostondemand/library/

- IBM Product Publications for AS/400

  http://as400bks.rochester.ibm.com

- Netscape Object Signing

  http://developer.netscape.com/docs/manuals/signedobj/trust/index.htm

- Netscape Preference Wrangler

  http://developer.netscape.com/library/technote/security/prefwrangler.html

- Netscape Security Preferences for Communicator

  http://developer.netscape.com/library/technote/security/sectn3.html
- Netscape Directory server

  http://enterprise.netscape.com/products/identsvcs/directory.html
- Netscape's SSL home page

  http://home.netscape.com/eng/ssl3/ssl-toc.html
- Java security tools summary

  http://java.sun.com/docs/books/tutorial/security1.2/summary/tools.html
- Get Java software

  http://java.sun.com/getjava/download.html
- Java Policy File Creation and Management Tool

  http://java.sun.com/j2se/1.3/docs/tooldocs/win32/policytool.html
- The Sun Microsystems product home page

  http://java.sun.com/products/
- The Swing Connection: Mixing Heavy and Light Components

  http://java.sun.com/products/jfc/tsc/articles/mixing/index.html
- Java Web Start Documents

  http://java.sun.com/products/javawebstart/
- Java 2 Plug-in tutorial

  http://java.sun.com/products/plugin/
- Java Web Start 1.4.2 Developer Guide

  http://java.sun.com/j2se/1.4.2/docs/guide/jws/developersguide/contents.html
- Setting up the Remote Abstract Window Toolkit for Java on a remote display

  http://publib.boulder.ibm.com/pubs/html/as400/v4r4/ic2924/info/java/rzaha/devkit.htm
- iSeries Information Center

  http://publib.boulder.ibm.com/iseries/v5r1/ic2924/index.htm
- iSeries Information Center AS/400 NetServer

  http://publib.boulder.ibm.com/html/as400/v5r1/ic2924/info/rzahl/rzahlusergoal.htm
- IBM iSeries online documentation What's New

  http://publib.boulder.ibm.com/pubs/html/iseries/online/chgfrm.htm
- WebSphere Portal serve troubleshooting

http://publib.boulder.ibm.com/pvc/wp/current/ena/en/InfoCenter/wps/trouble.html

- WebSphere Portal release notes

  http://publib.boulder.ibm.com/pvc/wp/current/exp/en/InfoCenter/wps/release_notes.html

- How Internet Explorer Java Virtual Machine searches for classes

  http://support.microsoft.com/default.aspx?scid=kb;EN-US;q177168

- HOWTO: Make Your Java Code Trusted in Internet Explorer

  http://support.microsoft.com/default.aspx?scid=KB;EN-US;q193877&

- IBM - Fixes for Netscape Communicator on AIX

  http://techsupport.services.ibm.com/aix/efixes/netscape/

- IBM @server Support

  http://techsupport.services.ibm.com/eserver/fixes

- Adobe Acrobat Reader Asian font packs

  http://www.adobe.com/products/acrobat/acrrasianfontpack.html

- Troublshooting AS/400 SSL Enabled Telnet server

  http://www.as400.ibm.com/tstudio/tech_ref/tcp/telntssl/Index.htm

- IBM AS/400 TCP/IP Reference

  http://www.as400.ibm.com/tstudio/tech_ref/tcp/indexfr

- IBM AS/400 Download TELNET exit program files

  http://www.as400.ibm.com/tstudio/tech_ref/tcp/telex/telexdwn.htm

- Cryptanalysis of MD5 Compress

  http://www.cs.ucsd.edu/users/bsy/dobbertin.ps

- Novell Developer home page

  http://www.developer.novell.com

- IBM Developerworks, Java home page

  http://www.ibm.com/developerworks/java/

- IBM Developerworks, Java technology

  http://www.ibm.com/developerworks/java/jdk/index.html

- The IBM public IBM developer kit porting Web page:

  http://www.ibm.com/developerworks/java/jdk/?dwzone=java

- IBM Developerworks, Java developer kits

  http://www.ibm.com/developerworks/tools.nsf/dw/java-devkits-byname

- IBM AS/400 Support for Windows Network Neighborhood API Mini-Guide

  http://www.ibm.com/servers/eserver/iseries/netserver/apiminiguide.htm
- IBM Performance Management for IBM @server iSeries

  http://www.ibm.com/servers/eserver/iseries/perfmgmt/resource.htm
- IBM HTTP Server iSeries home page

  http://www.ibm.com/servers/eserver/iseries/software/http/services/apache.htm
- IBM Communications Server online library

  http://www.ibm.com/software/network/commserver/library/
- Communications Server for OS/390 white papers

  http://www.ibm.com/software/network/commserver/library/whitepapers/csos390.html
- IBM SecureWay Directory home page

  http://www.ibm.com/software/network/directory/
- IBM Software Networking and Communications Support home page

  http://www.ibm.com/software/network/support
- IBM WebSphere Software Support Bulletin

  http://www.ibm.com/software/network/support/alert
- IBM Personal Communications Web page

  http://www.ibm.com/software/pcomm/
- WebSphere Portals library

  http://www.ibm.com/software/webservers/portal/library.html
- WebSphere Portal Server troubleshooting

  http://www-3.ibm.com/software/webservers/portal/library/InfoCenter/wps/trouble.html
- The Internet Engineering Task Force home page

  http://www.ietf.org
- Internet Engineering Task Force RFC page

  http://www.ietf.org/rfc.html
- The Transport Layer Security (TSL) protocol

  http://www.ietf.org/rfc/rfc2246.txt
- TN3270 Enhancements

  http://www.ietf.org/rfc/rfc2355.txt?number=2355
- Microsoft to ship Sun's technology

http://www.microsoft.com/windowsxp/pro/evaluation/news/jre.asp

- Code Signing for Java Applets

  http://www.suitable.com/Doc_CodeSigning.shtml

- Thawte the global digital certificate authority

  http://www.thawte.com

- Verisign - Introduction to Cryptography

  http://www.verisign.com/client/about/introCryp.html

- Verisign - Introduction to Cryptography

  http://www.verisign.com/repository/crptintr.html

- IBM Software Internet Delivery

  http://www6.software.ibm.com/aim/home.html

How to get IBM Redbooks

Search for additional Redbooks or drafts, view, download, or order hardcopy from the Redbooks Web site:

http://www.ibm.com/redbooks

Also download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

Drafts are Redbooks in progress; not all Redbooks become Drafts and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the **CD-ROMs** button on the Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.

Index

Host Access Client Package V4 Update

Redbooks

(2.0" spine)
2.0" <-> 2.498"
1052 <-> 1314 pages

Host Access Client Package V4 Update

Web Express Logon and Web Start

ZipPrint added to HOD

New PCOMM features

The two products in the IBM Host Access Client Package, IBM Personal Communications, and IBM WebSphere Host On-Demand have been enhanced with new features and functions to keep up with current technologies. This IBM Redbook explores the features and functions of each product as it relates to deployment in today's rapidly expanding TCP/IP environment.

The following is an overview of many of the topics found in this redbook:
-Java Web Start for using HOD without a browser
-Web Express Logon for automated logon support
-Secure Shell (SSH) support for VT display sessions
-ZipPrint support
-Sharing and reusing macros and server macro library support
-Backup server support for clients
-Mac OS X emulator and database clients
-IPv6 support
-Personal Communications Windows Terminal Server support
-PCOMM connection timeout improvements
-PCOMM support for IPv6 Telnet connections
-PCOMM visual enhancements to OIA and poppad

SG24-6182-02 ISBN 0738498408