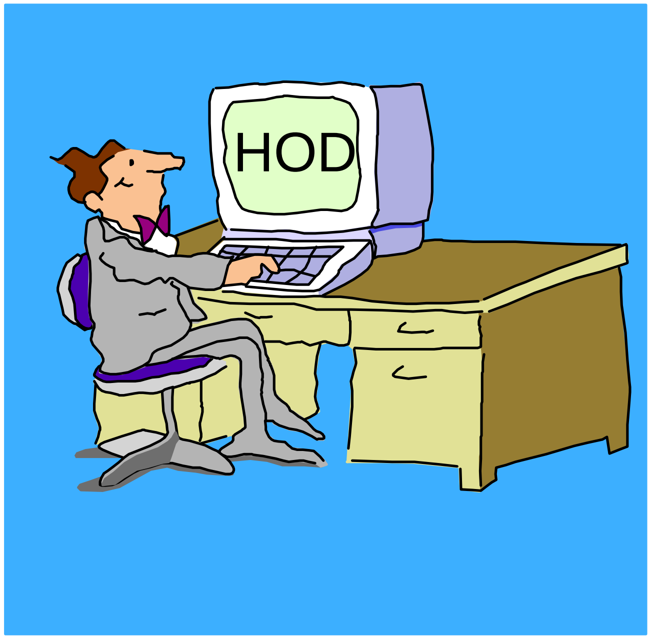
IBM SecureWay Host On-Demand V4 for OS/390

Overview and Implementation Issues



Linda Harrison
lharriso@us.ibm.com
Johnny Chi
chi@us.ibm.com
Robert Morse
rdmorse@us.ibm.com

Agenda

- OS/390 Host On-Demand Installation
  - Product Packaging
  - Installation... SMP/E and non-SMP/E
  - General Installation Hints and Tips and Other Gotchas
- OS/390 Host On-Demand Customization
  - CS for OS/390 Customization... Groups, Groups and more Groups
- OS/390 TN3270E Secure Sockets Layer (SSL)

Abstract

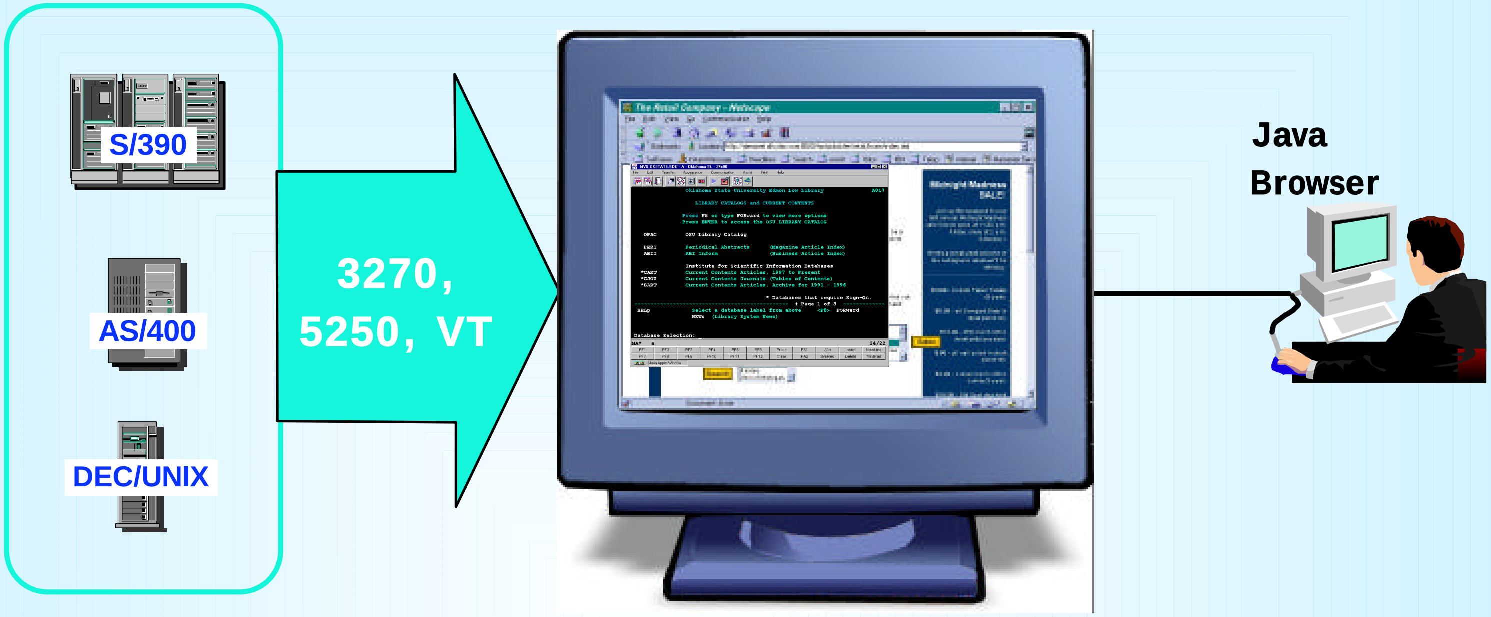
TITLE: OS/390 Host On-Demand, Version 4.0 and 4.0.1

PRESENTERS: Linda Harrison, Johnny Chi and Robert Morse, ATS Enterprise Networking Technical Support

AUDIENCE: OS/390 Host On-Demand Installers and Administrators

ABSTRACT: Host On-Demand's browser-based access is the simplest way ever for users to reach critical host data because the user is not required to load or configure any software. Host On-Demand is a JAVA enabled WEB based terminal emulation software supporting TN3270(E), TN5250, VT100 and VT220 terminals as well as 3827 and 5250 print emulation. For users, Host On-Demand helps eliminate the confusing host and port names as all of the configuration is easily provided by the Administrator. From a web browser, users just click on a hyperlink that launches a session with the host. In addition to the usual web access, any number of sessions can be launched with multiple hosts at the same time. Since Host On-Demand installs on a server, maintenance, distribution, and upgrades are simplified. In the case of OS/390 Host On-Demand, the server that Host On-Demand installs onto is the OS/390 system, where most of today's enterprise mission-critical information still resides.

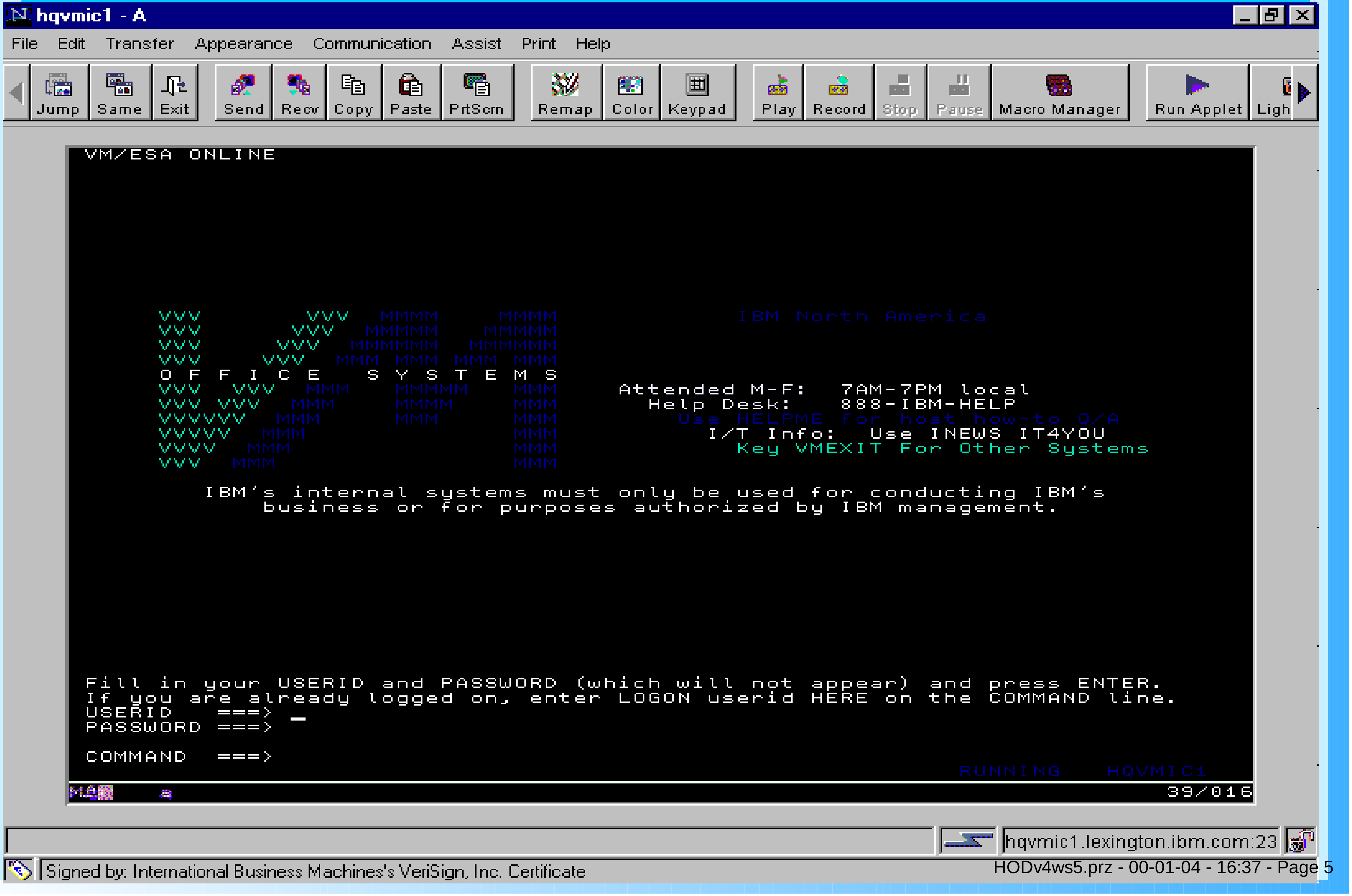
SecureWay Host On-Demand



Web-to-Host Terminal Emulation Solution

- **Extends host application reach to new users**
- **Reduces I/T costs through centralized installation and administration**
- **Supports client and server platforms of choice**
- **Requires no middle-tier runtime server**
- **Enables rapid host integration in new e-business applications**

Access Green Screen



```
VM/ESA ONLINE









     VVV        VVV  MMMM     MMMM              IBM North America
     VVV       VVV  MMMMM    MMMMM
     VVV      VVV  MMMMMM   MMMMMM
     VVV     VVV  MMM MMM MMM MMM
     O F F I C E   S Y S T E M S
     VVV  VVV  MMM   MMMMM   MMM        Attended M-F:   7AM-7PM local
     VVV VVV  MMM    MMMM    MMM          Help Desk:    888-IBM-HELP
     VVVVVV  MMM     MMM     MMM        Use HELPME for host how-to Q/A
     VVVVV  MMM              MMM              I/T Info:   Use INEWS IT4YOU
     VVVV  MMM               MMM                  Key VMEXIT For Other Systems
     VVV  MMM                MMM

        IBM's internal systems must only be used for conducting IBM's
            business or for purposes authorized by IBM management.









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   HQVMIC1
                                                                        39/016
```

Host Integration Product Positioning

Personal Communications is IBM's answer for host emulation

➡ Designed for customers with a wide variety of network protocols who need a powerful access product

- Tailored to client's operating system for high performance
- Enhanced desktop interfaces
- Rich set of APIs and reusable component for customized applications
- Registered user pricing model

Host On-Demand is IBM's answer for Web-based host emulation

➡ Especially designed for Intranet or Extranet access

➡ Provides central management solution for client software

- Requires Java enabled browser
- Users connect for extended periods of time
- Fast response times are important to maximize productivity
- Users are comfortable with traditional host green screens
- Full function emulation
- Rich set of APIs and reusable components for customized applications
- Concurrent user pricing model

e-business™

OS/390 Host On-Demand V4.0.x

Installation:

Product Packaging

e-business™

Product Packaging

➢ OS/390 Host On-Demand (5648-C54) V4.0.x Features

FMID	Description	Medium	Feature Number
HHOE40F (V4.0.1+ only)	TDES US/CAN English (168-bit encryption*)	9/6250 tape	6732
		3480 cart	6733
		4mm cart	6738
HHOE40S	DES US/CAN English (128-bit encryption*)	9/6250 tape	5439
		3480 cart	5440
		4mm cart	5441
HHOE40W	Int. English (40-bit encryption)	9/6250 tape	5443
		3480 cart	5444
		4mm cart	5445

*** Subject to Export Regulation**

Software Requirements

Minimum OS/390 Software Requirements

Program Number	Product Name and Minimum VRM/Service Level	Install Requirement
5647-A01	OS/390 Version 2 Release 5	Yes
5655-A46	Java for OS/390 V1.1.6 with APAR OW38252 (see http://www.s390.ibm.com/java)	No
5697-D43	Domino Go Webserver for OS/390 V5R0M0	No

Notes:

- The OS/390 Communications Server TCP/IP Services and Unix Systems Services, both included with OS/390, are required by all FMID's of IBM SecureWay Host On-Demand V4.0.x for OS/390 at run time.
- A PTF representing Corrective Service Diskette (CSD) 1 for Host On-Demand V4.0.1 has been incorporated into the product tape for FMID HHOE40F. A separate PTF tape representing CSD 1 is available for FMID's HHOE40S (APAR OW40500 PTF UW62175) and HHOE40W (APAR OW40501 PTF UW62622).

Software Requirements (cont.)

- CSD 1 PTF tape was created as a NO LABEL tape with blocksize of 12960.
- After unloading CSD 1 or 2 PTF tape the shell script hod40ptf.sh must be run to un-tar the PTF to replace the changed files.
- A PTF tape representing CSD 2 is available for FMID's HHOE40F (APAR OW41854 PTF UW64905), HHOE40S (APAR OW41853 PTF UW64945), and HHOE40W (APAR OW41852 PTF UW65002).
- HOD V4.0 base code must be installed before an SMP/E install of CSD 2 but CSD 1 is not required. CSD 2 contains all of the updates from CSD 1 as well.
- HOD V4.0.1 supports Screen Customizer 1.0 (ordered seperately).
- HOD V4.0.2 supports Screen Customizer 1.0.1 (ordered seperately).

HOD on OS/390

- **OS/390 version 2 releases 4, 5, 6, and 7 all came with HOD V1.**
- **HOD v3 Entry is available via the web at URL:**

http://www.ibm.com/software/enetwork/hostondemand/downloads

- **Announcement Letters for each version of HOD:**

  HOD v2 Announcement Letter 298-064

  HOD v3 Announcement Letter 298-331

  HOD v4 Announcement Letter 299-204

HOD V3 Entry

- **HOD V3 Entry is a subset of HOD V3.**
- **Compared to HOD V1, HOD V3 Entry offers the following additional features:**

  TN5250 & VT 52/100/220 support

  Copy / Cut / Paste

  Persistent Browser Caching

  Print Screen

  National Language Support

  Eurocurrency support

HOD V3 Entry (cont.)

- **Compared to HOD V3, HOD V3 Entry lacks:**

Host connectivity through non-IBM TN gateways.

(HOD V3 Entry will be restricted to being used with IBM Communications Server server that it was installed upon.)

10 concurrent sessions (HOD V3 entry only offers 2)

Color Mapping

Run Applet

Macro Record / Play

Graphical User Interface

User & Group Configuration

Thin Client Option

File Transfer (IND$FILE & Database On-Demand)

Host Print

(cont.)

HOD V3 Entry (cont.)

- **Compared to HOD V3, HOD V3 Entry lacks (cont.):**

  Host Access Class Libraries

  Java Beans

  TN3270E support (LU Pools & NVT)

  SSL Encryption

HOD Function

Function	HOD V1	HOD V2.0	HOD V3.0	HOD V3.0 Entry	HOD V4
Emulation Types					
TN3270	Yes	Yes	Yes	Yes	Yes
TN5250		Yes	Yes	Yes	Yes
VT 52/100/220		Yes	Yes	Yes	Yes
No. of Sessions	2	Unlimited (10)	Unlimited (10)	2	Unlimited
User Interface					
Graphical Toolbar	Yes	Yes	Yes	Yes	Yes
Keypad	Yes	Yes	Yes	Yes	Yes
Auto Font Sizing	Yes	Yes	Yes	Yes	Yes
Keyboard Mapping	Yes	Yes	Yes	Yes	Yes
Color Mapping			Yes		Yes
Copy / Cut / Paste		Yes	Yes	Yes	Yes
Run Applet		Yes	Yes		Yes
Macro Record / Play			Yes		Yes
ResQ!Net/LE (Default GUI)			Yes		Yes
ResQ!Net Customizable GUI			Yes (Separate)		Yes (Separate)

e-business™

HOD Function (cont.)

Function	HOD V1	HOD V2.0	HOD V3.0	HOD V3.0 Entry	HOD V4
Configuration					
Guest (Default Config.)	Yes	Yes	Yes	Yes	Yes
Individual User Config.		Yes	Yes		Yes
User Group Config.			Yes		Yes
Persistent Browser Caching		Yes	Yes	Yes	Yes
Flexibility of Applet Size			Yes		Yes
LDAP Support					Yes
File Transfer					
File Transfer (IND$FILE)		Yes	Yes		Yes
Database On-Demand (OS/400)			Yes		Yes
Print Support					
Convenience (Screen) Print		Yes	Yes	Yes	Yes
Host Print			Yes		Yes

HOD Function (cont.)

Function	HOD V1	HOD V2.0	HOD V3.0	HOD V3.0 Entry	HOD V4
Programming Support					
Host Access Class Library		Yes	Yes		Yes
Beans for Java			Yes		Yes
Host Access ActiveX Controls					Yes
Class Library (HACL)					Yes
Networking Support					
TN3270E LU Pool Support		Yes	Yes		Yes
TN3270E NVT Support			Yes		Yes
Choice of TN Server/Location		Yes	Yes		Yes
SSL Encryption & Server Auth		Yes	Yes		Yes
SSL Client Authentication					Yes
RAS (Tracing)	Yes	Yes	Yes	Yes	Yes

e-business™

HOD Function (cont.)

Function	**HOD V1**	**HOD V2.0**	**HOD V3.0**	**HOD V3.0 Entry**	**HOD V4**
Internationalization					
NLS (SBCS & DBCS)	US English	Yes	Yes	Yes	Yes
NLS (BiDi)			Yes	Yes	Yes
Eurocurrency Support			Yes	Yes	Yes
Improvements					
AS/400 5250 Host Print, etc.					Yes

OS/390 Host On-Demand V4.0.x:
SMP/E Installation

™

e-business

SMP/E Installation

- Two methods of Host On-Demand installation available
  - SMP/E
  - Non-SMP/E
- SMP/E traditional method of installation/removal of all software and maintenance on OS/390
  - Supports RAS
  - Auditable
  - Preferred method of installation of SecureWay Host On-Demand
- Non-SMP/E installation described separately

SMP/E Installation

Step	Description	Supplied Jobstream
1	Unload sample JCL from Product Tape and customize to conform to user standards.	See sec 6.1.4 of Program Directory
2	Perform SMP/E RECEIVE from Product Tape.	HOMRECVE
3	Allocate SMP/E Target and Distribution libraries.	HOMALLOC
4	Create SMP/E DDDEF entries. Note: If Host On-Demand is being installed on a Target system which is different then the Driver system there is an additional jobstep required in this step. (see sec 6.1.8 of Program Directory)	HOMDDDEF
5	Allocate HFS Note: This jobstream provides for an initial allocation of 460 cylinders of 3390 disk space. Experience indicates that a more appropriate value is approximately 900 cylinders for Host On-Demand V4.0 and approximately 1200 cylinders for V4.0.x. Note: See also step 6 on the next foil.	HOMHFS

SMP/E Installation

Step	Description	Supplied Jobstream
6	Copy Host On-Demand V2.0 or V3.0 HFS contents to V4.0 HFS. Note: This step is **only** applicable if you are migrating from an earlier release of Host On-Demand. It will unload the existing HFS, allocate a new HFS (expanded for V4) and reload the contents of the old HFS. Note: This sample jobstream suffers from the same dasd shortfall as does the HOMHFS jobstream in step 5 and needs to be adjusted accordingly. Note: Run step 5 or step 6 but not both depending on the situation (i.e. initial install vs. migration).	HOMCOPY
7	Logon to Unix System Services. Create HFS mountpoint (/usr/lpp/HOD) and mount Host On-Demand HFS created in either step 5 or 6 above. Note: The permission bits for the mountpoint must be set to (7,5,5).	n/a
8	Perform SMP/E APPLY CHECK followed by APPLY.	HOMAPPLY

e-business™

SMP/E Installation

Step	Description	Supplied Jobstream
9	Perform SMP/E ACCEPT CHECK followed by ACCEPT. Note: This step is optional at this point and can be performed later if desired.	HOMACCPT
10	Delete Host On-Demand V2.0 DDDEFs (if applicable).	HOMDDCLN
11	Logon to Unix System Services, cd to /usr/lpp/HOD and run the hod40mvs.sh shell script. Note: If migrating from a previous version release of HOD backup any modifications which the user has made in either /usr/lpp/HOD/ondemand/lib or /usr/lpp/HOD/ondemand/HOD and remove this directories (e.g. rm -Fr /usr/lpp/HOD/ondemand/lib). The instructions in the Program Directory indicate that this removal is automatic but this comment is incorrect. Failure to remove these directories may result in HFS space problems during install and cause the hod40mvs.sh script to fail.	n/a

SMP/E Installation

Step	Description	Supplied Jobstream
11 (cont.)	Note: The comments in the Program directory also indicate that migration of the user definitions contained in the /usr/lpp/HOD/ondemand/private directory is automatic. This is incorrect. The act of changing the default directory structure from /usr/lpp/HOD/ondemand to /usr/lpp/HOD/hostondemand between versions is not properly accounted for in the hod40mvs.sh script. If upgrading from a previous version/release therefore the user will need to manually copy his/her prior definitions following successful completion of the hod40mvs.sh script, e.g. cp /usr/lpp/HOD/ondemand/private/*.* /usr/lpp/HOD/hostondemand/private.	n/a
12	Update Web server "pass" rules and verify/update resource mapping (i.e. "addtype") directives. Note: Reference to updating the "addtype" parameters in httpd.conf was added to the Program Directory for V4.0.1. It is not present in the V4.0 Program Directory.	see sec 6.2.2 in Program Directory

e-business™

SMP/E Installation

Step	Description	Supplied Jobstream
13	Start Host On-Demand Note: Please see sec 6.2.3 in the Program Directory. The HOMSERVR started must be started from a RACF userid with root authority in OS/390 Unix System Services. Sec 6.2.3 indicates the necessary commands to provide this authorization. Note: HOMSERVR indirectly executes a shell script (ServiceManager.sh) located in the Host On-Demand HFS. If the mountpoint for the Host On-Demand HFS is not /usr/lpp/HOD (the default) then an update is required to the PARM passed on the HOMSERVR PROC's EXEC statement. Note: Lastly... (You thought we'd never get here didn't you.) The ServiceManager.sh script will generally require updates to either the CLASSPATH, or PATH or both variables depending on the manner in which JAVA has been installed. The script is commented to indicate the required changes.	HOMSERVR

SMP/E Installation

Step	Description	Supplied Jobstream
14	There is no step 14! Host On-Demand should now be up and running and ready for the Administrator.	n/a

e-business™

OS/390 Host On-Demand V4.0.x:
Non-SMP/E Installation

e-business™

Non-SMP/E Installation

- Alternative approach to SMP/E install
    - Utilizes the readily available Host On-Demand product CD
    - Does not require a program tape
    - Generally undocumented
        - Program Directory will be included in softcopy on the Host On-Demand product CD in a future release to address this issue.
- As noted previously... SMP/E preferred method of installation of SecureWay Host On-Demand

Non-SMP/E Installation

Step	Description
1	Allocate a target Host On-Demand HFS as described previously under SMP/E installation. Note: HFS size should be approximately 900 cylinders for Host On-Demand V4.0 and approximately 1200 cylinders for Host On-Demand V4.0.x.
2	Logon to Unix System Services. Define a mountpoint (e.g. /usr/lpp/HOD), set the permission bits to (7,5,5) and mount the target Host On-Demand HFS.
3	Insert the Host On-Demand CD into the CDROM drive of an available Windows 95, 98 or NT workstation.
4	Exit from the automatic install process if it initializes and view the CD with Windows Explorer. The \tar directory on the CD will contain (among others) the following files: ▸ HOD40MVS.SH ▸ HOD40MVSCD.TAR.Z ▸ HOD40SRV.TAR.Z, and ▸ HOD40WWW.TAR.Z

Non-SMP/E Installation

Step	Description
5	Now FTP to the target OS/390 Host On-Demand system and put the four previously noted files into the Host On-Demand HFS mounted at /usr/lpp/HOD. Note: Filenames on the CD are in upper case. The FTP put commands must allow for this and the resulting filenames on OS/390 must be in lower case. E.g. ▸ "put HOD40MVS.SH hod40mvs.sh" Note: HOD40MVS.SH represents the install shell script and must be transferred in ASCII which will allow it to be translated to EBCDIC on receipt by the OS/390 FTP server. The remaining three tar files must be transferred in BINARY mode. Note: When transferring the three tar files all names should be folded to lower case with the exception of the ending "Z" which should be left in upper case. E.g. ▸ "put HOD40MVSCD.TAR.Z hod40mvscd.tar.Z"
6	Logon to Unix System Services, cd to /usr/lpp/HOD and run the hod40mvs.sh install shell script with the "eval" option as follows: > hod40mvs.sh eval

Non-SMP/E Installation

Step	Description
7	Following the remaining SMP/E procedures/comments as outlined previously in steps 11-14.

OS/390 Host On-Demand V4.0.x Other Documentation and Installation "Gotchas"

Documentation and Installation "Gotchas"

- The V4.0.x Program Directory does not indicate the cumulative maintenance status of V4 vs. V2 or V3. V4.0 represents a rollup of applicable maintenance through V3 CSD3.
- The Program directory for V4.0 does not sufficiently highlight the change in product install directories sufficiently (i.e. from /usr/lpp/HOD/ondemand to /usr/lpp/HOD/hostondemand). This has been addressed in V4.0.1. As a result. if migrating from a previous version/release, a customer may miss a required update to previously existing "pass" statements in his/her httpd.conf file.

e-business ™

Documentation and Installation "Gotchas"

- Documentation for HOD V4.0.x is provided in softcopy only. The following URL's can be used once Host On-Demand is installed (per the instructions in the Program Directory) and is up and running.
  - HOD V4.0 and V4.0.1:

    http://hod_server_name/hod/en/doc/readme/readme.html

    http://hod_server_name/hod/en/doc/install/install.html

    http://hod_server_name/hod/en/doc/beans/API_users_guide.html

    http://hod_server_name/hod/en/doc/hostprint/hostprint.html
  - HOD V4.0.2:

    http://hod_server_name/hod/en/doc/readme/readme.html.ascii

    http://hod_server_name/hod/en/doc/install/install.html.ascii

    http://hod_server_name/hod/en/doc/beans/API_users_guide.html.ascii

    http://hod_server_name/hod/en/doc/hostprint/hostprintref.html.ascii
- Note: hod_server_name represents the TCP/IP hostname or IP address of the OS/390 system on which Host On-Demand has been installed.

Documentation and Installation "Gotchas"

- The documentation, including the Program Directory, is now available from the web page (select Library).

  http://www.software.ibm.com/network/hostondemand

- Following installation, the tar files in the /usr/lpp/HOD directory are no longer of use and can be backed up and deleted to free up HFS space if desired.

OS/390 Screen Customizer

e-business

Install Screen Customizer Client

- **Only the Screen Customizer "Client" is supported on OS/390.**

Step	Description
1	FTP the **mvscli.tar** and **mvsdoc.tar** files from the /tar directory on the Screen Customizer Client CD to the OS/390 Host On-Demand server /usr/lpp/HOD directory. Transfer in binary.
2	On OS/390 change to the HOD *publish* directory (/usr/lpp/HOD/hostondemand/HOD is the default): **cd /usr/lpp/HOD/hostondemand/HOD**
3	Untar and install the Client files into the HOD *publish* directory: **tar -xf /usr/lpp/HOD/mvscli.tar**
4	Untar and install he documentation files: **tar -xf /usr/lpp/HOD/mvsdoc.tar**

Copy Custom Files

- **After installing Screen Customizer Client, copy customized files from a Windows Scren Customizer Administrator to OS/390.**

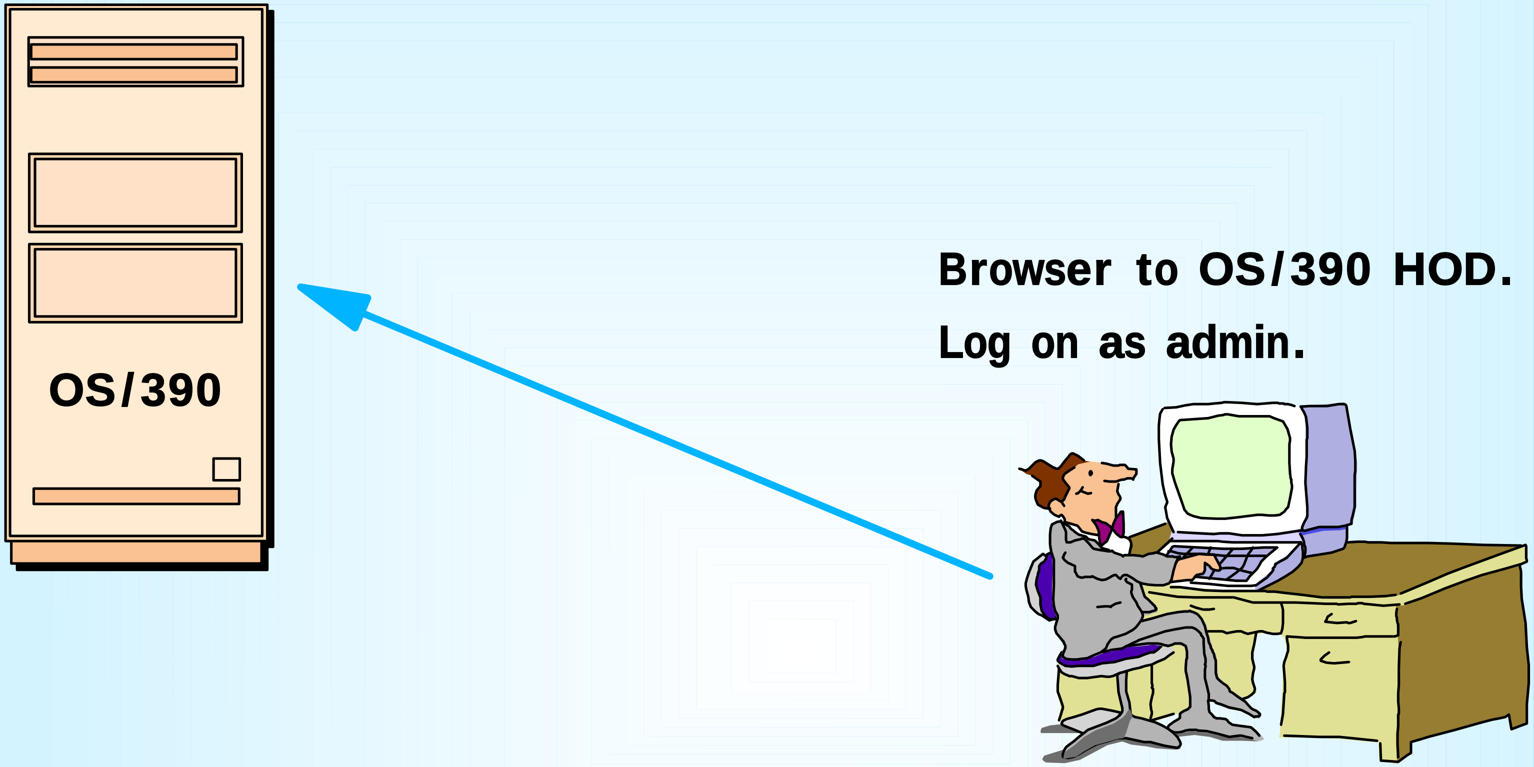
Step	Description
1	On OS/390 create five subdirectories in the *publish*/custom directory: **/usr/lpp/HOD/hostondemand/HOD/custom/1st** **/usr/lpp/HOD/hostondemand/HOD/custom/map** **/usr/lpp/HOD/hostondemand/HOD/custom/ps** **/usr/lpp/HOD/hostondemand/HOD/custom/ref** **/usr/lpp/HOD/hostondemand/HOD/custom/wsp** Set the permission bits to (7,5,5) for all subdirectories.
2	FTP the files of each corresponding subdirectory on the Windows Administrator to the OS/390 host in the *publish*/custom direcotry. Files must be transferred in binary.

OS/390 Host On-Demand Administration

™

e-business

Host On-Demand Administration



Browser to OS/390 HOD.

Log on as admin.

Create groups (or use default HOD group).

Create sessions for groups.

Create users and assign them to groups.

Create specific sessions for individual users as necessary.

Host On-Demand Administration

- Essentially the same as for all other Host On-Demand server platforms:
  - Connect to HOD server

    e.g. http://hod_server_name/hod/HODMain.html
  - Select Administration and logon as admin/password
  - Once logged on:

    create groups

    create sessions (e.g. 3270, 5250, VT100, etc.) for groups

    create users and assign them to groups

    create specific sessions for individual users as necessary.

Host On-Demand Administration

- Every user must be a member of at least one group
  - When NOT using LDAP, a user may be a member of multiple groups in which case he/she will inherit the sessions associated with all of the groups to which they belong.
  - When using LDAP, a user may only be a member of one group.
- Tool for bulk creation of users, group, and sessions:

  http://poggly1.raleigh.ibm.com/dirutil/dirutil.html

e-business™

Host On-Demand Administration

- One potential issue exists if users are allowed to define their own sessions or modify inherited sessions:
  - A user who modifies a session inherited from a group level definition now has a local "instance" of that session. This may present a help desk problem since neither the help desk nor the user can differentiate the two sessions should the user subsequently have reason to call in for assistance. A suggestion has been made to HOD development that session icons be color coded in some way to indicate the owning "level", i.e. user, group, etc.

e-business™

CS for OS/390 IP Customization

e-business

Host On-Demand Customization

PROFILE TCPIP BEGINVTAM STATEMENT

PORT xxxx -define which telnet port the BEGINVTAM effects

HNGROUP -define group of hostnames (available in OS/390 v2r7 and above)

IPGROUP -define group of ipaddrs

LUGROUP -define group of LUs

LUMAP -map LU or LUGROUP to hostname, HNGROUP, ipaddr, or IPGROUP and optionally associate a printer LU or PRTGROUP

PRTGROUP -define group of printer LUs

PRTMAP -map printer LU or PRTGROUP to hostname, HNGROUP, ipaddr, or IPGROUP

HOD Session Customization

Destination Port

TN3270E -required for LU or LU Pool specification

LU or LU Pool

Associated Printer Session

e-business™

Host On-Demand Customization

PROFILE TCPIP BEGINVTAM STATEMENT

```
PORT 223
HNGROUP
   HNAMES1 andyh.washington.ibm.com patb.washington.ibm.com ENDHNGROUP
HNGROUP HNAMES2 **.bet.ibm.com ENDHNGROUP
IPGROUP IPNAMES1 255.255.240.0:9.82.0.0 ENDIPGROUP
IPGROUP IPNAMES2 9.82.130.4 9.82.1.161 ENDIPGROUP
IPGROUP IPNAMES3 255.255.224.0:9.82.128.0 ENDIPGROUP
IPGROUP IPNAMES4 9.82.1.2 9.82.1.10 ENDIPGROUP
LUGROUP NONHOD1 TCP20001..TCP20010 ENDLUGROUP
LUGROUP NONHOD2 TCP20011..TCP20020 ENDLUGROUP
LUGROUP HODLUG2 TCP20H01..TCP20H02 ENDLUGROUP
LUGROUP HODLUG3 TCP20H11..TCP20H20 ENDLUGROUP
LUGROUP HODLUG4 TCP20H21..TCP20H22 ENDLUGROUP
PRTGROUP PRTLUS1 TCP20P01..TCP20P10 ENDPRTGROUP
PRTGROUP PRTLUS2 TCP20P11..TCP20P12 ENDPRTGROUP
PRTGROUP PRTLUS4 TCP20P21..TCP20P22 ENDPRTGROUP
```

Host On-Demand Customization

```
PRTMAP PRTLUS1  IPNAMES1        ====> 1
LUMAP  NONHOD1  HNAMES1         ====> 2
LUMAP  NONHOD2  HNAMES2         ====> 3
LUMAP  HODLUG2  IPNAMES2 SPECIFIC PRTLUS2    ====> 4
LUMAP  HODLUG3  IPNAMES3        ====> 5
LUMAP  HODLUG4  IPNAMES4 GENERIC PRTLUS4     ====> 6
```

1 If a printer session is initiated to port 223 from any IP address in the 9.82.0.0 subnet (mask 255.255.240.0), the first available LU will be assigned between TCP20P01 and TCP20P10.

2 If andyh or patb from domain washington.ibm.com telnets into port 223, the first available LU will be assigned between TCP20H01 and TCP20H10.

3 If any host from domain bet.ibm.com or any sub-domain (including tomv.bet.ibm.com and suej.rustbuck.bet.ibm.com) telnets into port 223, the first available LU will be assigned between TCP20H11 and TCP20H20.

Host On-Demand Customization

4 If 9.82.130.4 telnets to port 223, and requests LU TCP20H01, it will be assigned, and a printer session with LU TCP20P11 will be initiated and associated with the host session. Likewise if 9.82.1.161 telnets to port 223, and requests LU TCP20H02, it will be assigned, and a printer session with LU TCP20P12 will be initiated and associated with the host session.

5 If any IP address in the 9.82.128.0 subnet (mask 255.255.224.0) telnets into port 223, the first available LU will be assigned between TCP20H11 and TCP20H20.

6 If 9.82.1.2 telnets to port 223, the first available LU will be assigned between TCP20H21 and TCP20H22, and a printer session with an LU between TCP20P21 and TCP20P22 will be initiated and associated with the host session. Likewise if 9.82.1.10 telnets to port 223, the first available LU will be assigned between TCP20H21 and TCP20H22, and a printer session with an LU between TCP20P21 and TCP20P22 will be initiated and associated with the host session. Where TCP20P21 is the printer LU if the host LU is TCP20H21, and TCP20P22 is the printer LU if the host LU is TCP20H22.

OS/390 TN3270E

Secure Sockets Layer (SSL)

e-business

Software Requirements (cont.)

Any one of the following optional OS/390 V2 elements is required if SSL support is desired.

- **Optional OS/390 IP Security Features required for SSL support**

Encryption Feature	V2R6	V2R7	V2R8	Elements
Base	HTCP350	HTCP370	HTCP380	SSL Authentication
Level 1	JTCP353, JTCP35T	JTCP373	JTCP383	Kerberos Non-DES IP Security CDMF IP Security SSL RC2/RC4
Level 2	JTCP352, JTCP35S, JTCP35L	JTCP372	JTCP382	Kerberos DES IP Security DES/CDMF IP Security SSL 56-bit SNMP CBC 56-bit DES
Level 3	JTCP35K	JTCP37K	JTCP38K	Kerberos DES IP Security Triple DES IP Security SSL Triple DES SNMP CBC 56-bit DES

Software Requirements (cont.)

- **Optional OS/390 IP Security Features SSL support provided**

Encryption Feature	SSLv2 Clients	SSLv3 Clients
Base	Not supported	NULL SHA NULL MD5 NULL NULL
Level 1	RC4 Export RC2 Export	RC4 MD5 Export RC2 MD5 Export NULL SHA NULL MD5 NULL NULL
Level 2	RC4 Export RC2 Export	DES SHA RC4 MD5 Export RC2 MD5 Export NULL SHA NULL MD5 NULL NULL
Level 3	Triple DES US DES US RC4 Export RC4 US RC2 Export RC2 US	Triple DES SHA US DES SHA RC4 MD5 Export RC4 SHA US RC4 MD5 US RC2 MD5 Export NULL SHA NULL MD5 NULL NULL

OS/390 TN3270E SSL

Create Public/Private Keys and Certificate Request

- The MKKF utility that ships as part of the OS/390 v2r6 and v2r7 LDAP server supports a 512-bit key size.

  To use MKKF with certification authority (CA) Verisign, APAR OW39793 is required and a password for the keyringfile has to be 6 to 8 characters.
- LDAP Security Server Feature JRSL161 (OS/390 v2r6) or JRSL171 (OS/390 v2r7) supports a 1024 key size.
- GSKKYMAN utility is part of OS/390 v2r8 System Secure Sockets Layer.

Server Authentication

Use the TELNETPARMS SECUREPORT statement to enable SSL Server Authentication.

For OS/390 v2r6 and r7, how to create a private key and server certificate in the server's key ring file and a password stash file using MKKF is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix D.

For OS/390 v2r8, how to create the Server key database using GSKKYMAN is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix C, and the Redbook "IBM SecureWay Host On-Demand: Enterprise Communications in the Era of Network Computing, SG24-2149".

On OS/390 v2r7 and r8 the TELNETPARMS ENCRYPTION statement specifies a subset of the supported encryption algorithms to use for a port.

Optional Client Authentication

On OS/390 v2r8 use the TELNETPARMS CLIENTAUTH statement to enable SSL Client Authentication.

Client certificate validation requires the root certificate for the Certificate Authority (CA) who issued the client certificate.

For RACF to check that the client has a RACF userid the certificate must be defined to RACF with the RACDCERT command.

RACF class SERVAUTH may be used to limit access on a port basis.

Create Certificate with MKKF

e-business

OS/390 v2r6 and v2r7 MKKF

Step	Description
1	Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in, and start MKKF: **mkkf**
2	Create and name Server Keyring file: **n**
3	Input the key ring filename or press Enter for the default keyfile.kyr filename.
4	'Work with keys and certificates': **w**
5	'Create a key pair and request a certificate': **c**
6	Input the key ring password.
7	Input password again for verification.
8	Select if the password will expire. To have the password expire, enter y, and the number of days until it expires. To have the password not expire, enter n.
9	Request a server certificate or a CA certificate: **s**

OS/390 v2r6 and v2r7 MKKF

Step	Description
10	Modify the key and certificate fields: **m**
11	Enter Key Name label.
12	Select Key Size.
13	Enter Server Name; fully-qualified hostname of the TN3270E server. If you select "Server Authentication" on your HOD session this Server Name must match the hostname in the DNS for the IP address of the TN3270E server.
14	Enter Organization Name.
15	Enter Organization Unit Name.
16	Enter Locality/City.
17	Enter State/Province.
18	Enter Postal Code.
19	Enter two digit Country Code: **US**
20	Create the key pair and certificate request: **r**

OS/390 v2r6 and v2r7 MKKF

Step	Description
21	Enter certificate request filename.
22	Exit Key menu: **x**
23	Create a stash file: **c**
24	Exit Key Ring menu: **x**
25	Save the key ring file and exit MKKF: **y**
26	If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, e-mail the certificate request to the CA and they will return it signed.
27	Start MKKF: **mkkf**
28	Open key ring file: **o**
29	Enter key ring filename from step 3.

OS/390 v2r6 and v2r7 MKKF

Step	Description
30	Enter password from step 6.
31	Receive certificate into the key ring: **r**
32	Enter certificate filename from step 21.
33	If you are receiving a self-signed certificate, confirm that you want to add the certificate to the key ring: **y**
34	If prompted, enter certificate label for the signed certificate.
35	Exit the Key Ring Menu: **x**
36	Save the key ring file and exit MKKF: **y**
37	Start MKKF: **mkkf**
38	Open the key ring: **o**

e-business™

OS/390 v2r6 and v2r7 MKKF

Step	Description
39	Enter key ring filename from step 3.
40	Enter password from step 6.
41	Work with keys and certificates: **w**
42	List the keys: **l**
43	Either select the key you want to make the default key: **s** Or display the next key: **n**
44	Make the key the default key in the key ring: **f**
45	Confirm default key: **y**
46	Exit the Key Menu: **x**

OS/390 v2r6 and v2r7 MKKF

Step	Description
47	Exit the Key Ring Menu: **x**
48	Save the key ring file and exit MKKF: **y**

49	Set up the environment for IKEYMAN:
	`export PATH=/usr/lpp/internet/bin:$PATH`
	`export LIBPATH=/usr/lpp/internet/bin:$LIBPATH`
	`export NLSPATH=/usr/lpp/internet/%L/%N:$NLSPATH`

50	Convert kyr file to kdb format: **`ikeyman -m -r keyfile.kyr`** where keyfile is the name of the mkkf key ring file from step 3.
51	Enter password from step 6. File keyfile.kdb is created.
52	Start IKEYMAN: **ikeyman**
53	'Open key database': **2**
54	Enter the key database name: **keyfile.kdb**

OS/390 v2r6 and v2r7 MKKF

Step	Description
55	Enter password from step 6 again.
56	'List/Manage keys and certificates': **1**
57	Select the number of the certificate you want to make available to HOD clients.
58	'Copy the certificate of this key to a file': **5**
59	Select binary file type: **2**
60	Input filename (ie. cert.der).

Create Certificate with GSKKYMAN

e-business

OS/390 v2r8 GSKKYMAN

Step	Description
1	Go to OMVS on OS/390, change the directory to the directory that you want the key database to be in. My directory on my system is /u/harrisl.
2	You can display your environment settings, including STEPLIB: **env** I needed to add the C and Crypto library to my STEPLIB: **`export STEPLIB=$STEPLIB:SYS1.CRYPTO.SGSKLOAD:SYS1.CPP.SCLBDLL`**
3	Start GSKKYMAN: **gskkyman**
4	'Create new key database': **1**
5	Input a database filename or press Enter for the default key.kdb filename. I input nm512.kdb and file ***/u/harrisl/nm512.kdb*** was created.
6	Input a password. I input *one0ssl* on my system.

OS/390 v2r8 GSKKYMAN

Step	Description
7	Input password again for verification.
8	Select if the password will expire. I selected *1* so that the password would expire. Then I pressed *Enter* to default to a 60 day expiration.
9	Select to work with the database now: **1**
10	If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, select 3 'Create new key pair and certificate request'. If you are going to create a self-signed certificate, select 5 'Create a self-signed certificate'. I created a self-signed certificate.
12	Select a version 3 Certificate: **3**
13	Input a certificate label name. I input *nmlow* for a certificate label name on my system.

OS/390 v2r8 GSKKYMAN

Step	Description
14	Select key size. I selected *1* for 512 key size.
15	Input 'Common Name'; the fully-qualified hostname of the TN3270E server. I input *mvsnm2*. If you select "Server Authentication" on your HOD session this 'Common Name' must match the hostname in the DNS for the IP address of the TN3270E server.
16	Input 'Organization'. I input *IBM*.
17	Input 'Organization'. I input *nsc*.
18	Input 'City'. I input *GBURG*.
19	Input 'State'. I input *MD*.
20	Input two digit 'Country'. I input *US*. Note: If you use USA then you get the following error when you try to save: Error: An asn.1 encoding/decoding error occurred.

e-business™

OS/390 v2r8 GSKKYMAN

Step	Description
21	Input number a days for certificate. I pressed *ENTER* to default to 365 days.
22	If you are purchasing a signed certificate, send the request to the CA and after the request is returned select 4 'Receive a certificate issued for your request'.
23	Set key as the default key in the database: **1**
24	Save the certificate to a file: **1**
25	Save as a binary file: **2**
26	Input a filename or press Enter for the default name of cert.crt. I input clow.crt and file ***/u/harrisl/clow.crt*** was created.
27	Do not exit yet: **0**
28	'Store encrypted database password': **11** I received a message back that the password had been stored in ***/u/harrisl/nm512.sth.***
29	Exit GSKKYMAN: **1**

Make Certificate Available to HOD Clients

e-business

OS/390 HOD SSL

Step	Description
1	Change to the root directory: **cd /**
2	Locate the HOD web-published directory: **find . -name WellKnown TrustedCAs.class*** The published directory on my system is /usr/lpp/HOD/hostondemand/HOD.
3	Copy the binary certificate into the published directory: **cp /u/harrisl/nmlow.crt /usr/lpp/HOD/hostondemand/HOD/nmlow.crt** Note: Copy as a binary file and no character conversion.
4	Locate the Host On-Demand server directory: **find . -name sm.zip*** The HOD server dir contains the file archives used to run the Service Manager. The server directory on my system is /usr/lpp/HOD/hostondemand/lib.
5	Change to the HOD published directory: **cd /usr/lpp/HOD/hostondemand/HOD**
6	Add the certificate to the CustomizedCAs.class file, using the keyrng JAVA utility. For HOD v3, type the following, all on one line: `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.sslight.tools.keyrng CustomizedCAs add --certificatetype cert.der` (continued on next page)

OS/390 HOD SSL

Step	Description
6 (cont.)	For HOD v4, type the following, all on one line: `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.hodsslight.tools.keyrng CustomizedCAs add --certificatetype cert.der` where HOD_SERVER_DIR is the HOD server directory, certificatetype is ca if you are adding a CA root certificate, or site if you are adding a site or self-signed certificate, and cert.der is the name of the file containing the binary certificate. Note: CustomizedCAs must be capitalized exactly as shown, there is a single hyphen before the classpath parameter, and a double hyphen before the certificate parameter. If the java command is typed in with the incorrect syntax you will get the following error: Unable to initialize Threads: Cannot find class /java/lang/Thread If no CustomizedCAs.class file exists, keyrng prompts you for a password with which to encrypt the new class-file. However, CustomizedCAs.class file must NOT be encrypted, so just press ENTER at the password prompt. (continued on next page)

OS/390 HOD SSL

Step	Description

6
(cont.)
	I found I needed the following path to the java code:
	`export PATH=$PATH:/usr/lpp/java/J1.1/bin`
	I found this in the ServiceManager.sh script in /usr/lpp/HOD/hostondemand/lib.
	I issued the following on my system:
	`java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\`
	`/usr/lpp/java/J1.1/lib/classes.zip \`
	`com.ibm.hodsslight.tools.keyrng CustomizedCAs add --site nmlow.crt`

7	Check to see if the certificate was added.
	For HOD v3, type the following, all on one line:
	`java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH`
	`com.ibm.sslight.tools.keyrng CustomizedCAs verify`
	For HOD v4, type the following, all on one line:
	`java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH`
	`com.ibm.hodsslight.tools.keyrng CustomizedCAs verify`
	(continued on next page)

OS/390 HOD SSL

Step	Description

7
(cont.)
	This should be followed by something similar to the following:
	
	------------------------ Key ring entry: 1 --------------------------
	        Entry type: Site Certificate
	            Key: RSA/512 bits
	          Subject: aix-f26.raleigh.ibm.com, ibm, US
	          Issuer: aix-f26.raleigh.ibm.com, ibm, US
	        Valid from: Fri Aug 13 2:21:29 EDT 1999
	          Valid to: Sun Aug 13 12:21:29 EDT 2000
	        Finger print: D7:2D:E9:6B:66:00:54:04:44:DE:02:E4:4E:1C:80:85
	
	The last certificate shown should be the one just added.
	I issued the following on my system:
	`java -classpath .:/usr/lpp/HOD/hostondemand/ibm/sm.zip: \`
	`/usr/lpp/java/J1.1/lib/classes.zip \`
	`com.ibm.hodsslight.tools.keyrng CustomizedCAs verify`

8	Exit OMVS.

OS/390 HOD SSL

Step	Description
9	Create HOD session with "Enable Security (SSL)" selected. Note: If you select "Server Authentication (SSL)" on your HOD session the 'Common Name' input when creating the certificate must match the hostname in the DNS for the IP address of the TN3270E server.

10	On OS/390 TN3270E server create TELNET SECUREPORT STATEMENT and BEGINVTAM PORT STATEMENT in TCPIP PROFILE:
	`TELNETPARMS`
	`   SECUREPORT 723 KEYRING HFS /u/harrisl/nm512.kdb`
	`   ...`
	`ENDTELNETPARMS`
	`BEGINVTAM`
	`   PORT 723`
	`   ...`
	`ENDVTAM`

11	Recycle HOD and TCP/IP servers and you're done!

Bibliography

e-business

Bibliography

- Program Directory for IBM SecureWay Host On-Demand for System/390:
  - GI10-3116-03 Version 4.0
  - GI10-3116-04 Version 4.0.1
  - GI10-3116-05 Version 4.0.2
- The following Redbook is available at http://www.redbooks.ibm.com:
  - IBM SecureWay Host On-Demand: Enterprise Communications in the Era of Network Computing, SG24-2149-01
- The following three documents are available after installation (where 9.82.1.100 is the IP address of the OS/390 system where HOD is installed):
  - Host On-Demand 4.0.1 Readme

    http://9.82.1.100/hod/en/doc/readme/readme.html
  - Planning and Installation Guide (also available in pdf as install.pdf)

    http://9.82.1.100/hod/en/doc/install/install.html
  - Host Access Beans for Java

    http://9.82.1.100/hod/en/doc/beans/API_users_guide.html
  - Host Printing Reference

    http://9.82.1.100/hod/en/doc/hostprint/hostprintref.html

Bibliography

- OS/390 Communications Server IP Configuration, SC31-8513
- OS/390 Cryptographic Services System Secure Sockets Layer Programming Guide and Reference, SC24-5877-01
- OS/390 Security Server (RACF) Command Language Reference, SC28-1919

Acknowledgements/Other Sources

™

e-business

Aknowledgements/Other Sources

- Host On-Demand Product Information site:
  - http://www.software.ibm.com/network/hostondemand

  Select Support from the above Home Page to get to the Support page.

  Select Library from the above Home Page to get to the Library page.

- Other sources for this presentation:

  Chip Mason - Sales Presentation

  Robert Morse - ENTS Networking Lab, Gaithersburg, MD.

- This document is available as presentation PRS162 on web site:
  - http://www.ibm.com/support/techdocs