

Welcome to IBM Host On-Demand Version 7 Help



Help is available from all IBM Host On-Demand windows.

You can access help in these ways:

- Click Help in a window.
- Click Table of Contents or Index from the host session Help menu.
- Click the question mark located on the top, right corner of the Administration window.

Click any topic in the navigation area to the left to locate information by keywords.

See *Planning, Installing, and Configuring Host On-Demand* for basic steps to configuring and starting Host On-Demand.

When you see this icon in the help: **The associated information:**



Returns to welcome screen and displays this information (how to use help).



Applies only to the Host On-Demand server.



Supplements important points in the main text.



Provides hints to help apply the techniques and procedures described in the main text.



Specifically relates to Lightweight Directory Access Protocol (LDAP) directory service.

Basic Configuration Steps



After installing Host On-Demand, you'll need to configure Host On-Demand sessions for your users. To do this, you need to create HTML files that define how users access session configuration information. You can use the Deployment Wizard to do this. See [Configuring Host On-Demand emulator clients](#) for information on using the Deployment Wizard to create HTML pages to launch Host On-Demand sessions.

Configuring the Host On-Demand Configuration Server

If you are using the configuration server-based model or the combined model to create HTML pages in the Deployment Wizard, you must configure sessions on the configuration server. The configuration server is configured through the Administration Utility. Complete the following steps to define sessions in the configuration server:

1. **Open the [Administration Utility](#).**

On Windows NT, 2000, or XP, click Start > Programs > IBM Host On-Demand > Administration > Administration Utility (or click the link above). On other platforms, open HODAdmin.html in the HOD directory. You can open the Administrator window from any computer that has access to the Host On-Demand server.

2. **Logon.**

The default user ID is *admin* and the password is *password*.

3. **Change your administrator password.**

For security reasons, you should change the default administrator password.

1. Click the Users/Groups.
2. Right-click admin from the User List, and click Properties.
3. Type the new password in the New Password box, and Confirm Password fields.
4. Click OK.



At this point, you may want to enable Host On-Demand to use Lightweight Directory Access Protocol ([LDAP](#)), which allows for information sharing between Host On-Demand servers. For instructions on how to setup and use this optional feature, click [here](#).

4. **Add groups.**

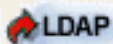
Host sessions can be defined for groups. Using groups can significantly reduce administration effort as all sessions defined for the group are available to all user IDs in the group.

1. Click New Group.
2. Type the Group ID. The first character must be a letter and you can use only A-Z, a-z, 0-9, . (period), and - (hyphen). Group IDs are converted to uppercase characters.



Group IDs are not converted to uppercase when you are using LDAP.

3. Optionally, type a description of the group. Any character is allowed except | (vertical bar) or # (number or pound sign).
4. Optionally, select the users who are to be members of the group from the **Not a member of** list.



If you are using LDAP, select the parent group from the **Subgroup of** list.

5. Click Add.



If you are using LDAP, skip this step.

6. Click Apply. Repeat steps 3 - 7 if you want to create another group.

7. Click Close when you finish.

5. **Add users.**

This step is only necessary if you are using the configuration server-based model.

Each user must have an ID to log on to Host On-Demand. This step describes how to create a user ID for each user. Optionally, if your users log on to a Windows domain, you can have the configuration server automatically create IDs for them based on their Windows usernames. This option is available through the Deployment Wizard, and does not require that you follow these steps to create user IDs.

1. Click New User.
2. Type the User ID. You can use only A-Z, a-z, 0-9, . (period), and - (hyphen). User IDs are converted to lowercase characters. IDs must be unique. You cannot have a user ID and a group ID that are the same, even if one is in lower case and the other is in upper.



User IDs are not converted to lowercase when you are using LDAP.

3. Optionally, type a description of the user. Any character is allowed except | (vertical bar) and # (number or pound sign).
4. Optionally, type a password and confirm it. Any character is allowed.
5. Select one or more groups for the new user from the **Member of** list. A 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.

6. If you do not want the user to change the password, click **User cannot change password**.
7. Click Apply. Repeat steps 2 - 7 if you want to create another user account.
8. Click Close when you finish.

To allow users to create accounts for themselves or for other users, check [Allow users to create accounts](#) on the Users/Groups window.

6. **Configure host sessions for users and groups.**

7. Right-click the user or group for whom you want to create a session and select Sessions.
8. In the Configure box, click the display or printer session you want to create.
9. On each tab, type or select the required information.
Check Lock to prevent users from changing the associated value. When this box is checked, users see a field value, but cannot change it.
10. Click OK.
11. To change the session's runtime properties, such as keyboard mapping, colors, or macros, right-click the session and select Start Session. Make the changes as a user would customize his session. You can only change the session's runtime properties if you downloaded the Full administration client. For more information about the Full administration client, see [Administration clients](#).

Depending on your environment, you may also need to configure additional services in the configuration server. To learn more about these features, click the following links:

[Firewalls](#)

[Security](#)

[LDAP](#)

[Database On-Demand](#)

[Redirector](#)

[License use count or license use management](#)

Logging on as an administrator



To log on for the first time after the initial installation:

1. Type the default user ID: **admin**.
2. Type the default password: **password**.
3. Click Log On.

If you have logged on before, enter the current user ID and password.

The system administrator can:

- Perform local or remote administration of the Host On-Demand Server.
- Configure, start, stop, and run traces of the Redirector or other services.
- Create and manage group and user accounts to control access to Host On-Demand and Database On-Demand.
- Create, change and delete host-session configurations for groups and users.
- Configure Host On-Demand to use Lightweight Directory Access Protocol (LDAP) to store user, group and session configuration data.
- Select the server to use for license usage reporting.
- Change the administrator's user ID and password.
- View the message-logs and traces of host sessions and the Redirector.



Managing users and groups



To manage users and groups, select Users/Groups in the Administration window.

As an administrator, you can create accounts for users or [allow users to create accounts](#).

The Users/Groups window enables you to manage user and group accounts for Host On-Demand and Database On-Demand. A tree view of the defined groups and users is displayed. To see the members of a group, select the group. To see only certain members of a group, use the filter by removing the check mark from Disable User Filter. Once the filter is enabled, the Filter window appears when you select a group. Choose to display all users in a group or only users matching the specified filter. For example, to display all users with IDs that begin with an L, enter L* in the UserID field and click Filter.

Right-click a user or group and select a task from the list.

[Creating a group](#)

[Configuring a host session for a user or group](#)

[Creating a user account and adding the user to a group](#)

[Copying a user or group](#)

[Changing a user's or a group's account](#)

[Deleting a user or group](#)

[Viewing a trace of a user's session](#)

[Changing the administrator user ID and password](#)

[Enabling users to create their own accounts](#)

Managing accounts

Access to Host On-Demand and Database On-Demand function is managed according to user and group accounts. User accounts contain specific information regarding a particular user, including the user's ID, password, description, group membership, database statements, and the host sessions that will be available to the user or group. By defining a group account, you can apply access settings to all users assigned to the group, making user management more efficient and more flexible. In this way, a host session can be defined once for a group and then made available to the group's members. Of course, a host session can still be defined for an individual user, in addition to sessions already defined for the user's group.

As an administrator, you can:

- Create, change, copy, and delete users and groups
- Allow users to create new user accounts
- Define host sessions for users and groups
- View trace information for users

User accounts

User accounts provide password-protected access to Host On-Demand and Database On-Demand. As part of the account, session configuration information is saved, along with changes that the user makes during a session, such as changes to keyboard and color mapping or recorded macros. Also, any changes to the Host On-Demand user desktop are saved (such as, adding new sessions and deleting sessions). No changes are saved if **Do Not Save Preferences** is checked.

Group membership

You can arrange users into groups. A user must be a member of at least one group but can be a member of several. In the latter case, the user will have access to the host sessions and database statements that are assigned to all the groups of which the user is a member.



If you are using Lightweight Directory Access Protocol (LDAP), then you can only be a member of one group. However, you can nest the groups, that is, include a group within a group.

Default group (HOD)

If you are using Host On-Demand for the private data store (instead of LDAP), the default group HOD, is supplied. You can change its Description and add users to it but you cannot change its name or delete it. If you are using LDAP, you can delete the HOD group, because LDAP treats the HOD group just like any other group. If you upgrade from Host On-Demand 2.0, the users are added as members of this group and their 2.0 sessions are converted to the 6.0 format and added to their 6.0 accounts. However, these sessions are available only to the users that own them, not to all members of the group.

Upgrading from Host On-Demand 3.0

If you have upgraded from Host On-Demand 3.0, you can continue to use the 3.0 user and group accounts, sessions and preferences, which are held in files in the `private` subdirectory of the Host On-Demand root directory. The `private` directory is not removed when you install the new version but you must make sure that it is in the correct place, based upon the following:

The default root directory in 3.0 was `ondemand` but, for 6.0, it is `hostondemand`. If you have installed 6.0 in the original (3.0) root directory, you need do nothing more. However, if you have installed 6.0 in a different root directory, you must move the `private` directory to the new root directory.

Host On-Demand 2.0 group (HOD2)

If you upgrade from Host On-Demand 2.0, icons for the **default** sessions from 2.0 are migrated and their icons appear in the HOD2 group's Configured Sessions window. You can use the sessions without change; however, you might want to take advantage of the new features by modifying the configurations. The HOD2 group does not have any members at first but you can [add them](#) in the usual way.

Administrator account

An Administrator account is provided. The default user ID is **admin** and the password is **password**. As an administrator, you can change the password but you cannot change the user ID and you cannot delete this account. We recommend that you change the password for security reasons.

Host sessions

You can configure host sessions for groups or for individual users. It is preferable to define groups, including their host sessions, then add users to the groups. All the users in the group then have access to the sessions defined for the group and you do not need to define sessions separately for each user. Users can customize their own sessions without affecting the session definitions in the groups, for example, change the screen colors, remap the keyboard, or hide the toolbar. Administrators can also customize these session definitions for a user or an entire group if the Full administration client is installed. For more information about the Full administration client, see [Administration client](#). If you change a user's session, the next time the user starts the session, the preferences will be active. If you change the group sessions, the user will inherit those changes, unless they have already customized those fields that are changed.

If you don't want users to be able to make changes to the sessions, click Lock in the session configuration window next to the fields you want to lock. Locking fields locks the startup values for a session. Users cannot change values for those

fields because the fields are unavailable.

You can also [disable functions](#) that you do not want users to access. You can disable any of the graphical interface items on pop-up menu and buttons in the Client window, the session menu, and the session toolbar. Disabling functions is different from locking functions. You can lock the fields of a function when you are configuring a session. Functions can be disabled when configuring a user or group. 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.

Shared user accounts (Guest log on)

There is no specific Guest user ID built into Host On-Demand. However, you can create a user ID (or more than one) that can be shared by multiple people. To do this, create a user ID and click **Do not save preferences** in the Create User window so that shared users can access the sessions provided for them, and can make changes that will be active only until they log off. If you do this, changes made by one user will not affect others. Of course, you can use the group feature to create groups for shared users by department or area, for example. You might also want to check the **User cannot change password** check box for your guest ID or, don't set a password at all.

User preferences

Unless **Do not save preferences** was checked when the account was created, preferences set during a host session are saved. These include color and keyboard mapping, macros created or changed, and the settings for the toolbars. These preferences are saved in the account of the individual user and associated with the icon for the session to which they apply. As a result of this:

- If a user changes the keyboard or color mapping during a session, the change applies only to that session or to copies of that session that are created after the change was made. The same is true for any macros that a user creates or changes during a session. For example, if a user creates a macro to transfer some files during a session named LONVM3, that macro cannot be used by a session named BIRMVM unless the latter is a copy of the former and was made after the macro was created. Also, the macro cannot be used by anyone else.
- If an administrator remaps the keyboard when configuring a session, the changed layout becomes the default for everyone who uses that session. If a user makes further changes when using the session, those changes apply only to that user, not to everyone. The differences between the default settings and the user's settings are saved in the user's account.
- If the user customizes a given field, those changes are saved in the user's account. When the administrator changes the default configuration, the user's default configuration is updated the next time the user logs on. The final configuration for the user is a combination of the new default configuration values and the user's settings. Generally, user settings replace the default configuration, unless the administrator locks a parameter so the user cannot change it.

Related topics

- [Creating your own user account](#)
- [Storing default session configurations and user preferences](#)



Adding or changing a group



To change a group, right-click the group and select Properties.

To add a group:

1. Click Users/Groups in the Administration window.
2. Click New Group.
3. Type the Group ID. The first character must be a letter and you can use only equivalent to English A-Z, a-z, 0-9, . (period), and - (hyphen). When using LDAP, Group IDs can be in mixed case. When using Host On-Demand to store configuration information, Group IDs are converted to uppercase characters.
4. Optionally, type a description of the group. Any character is allowed except | (vertical bar) or # (number or pound sign).



If you are using LDAP, select the parent group from the **Subgroup of** list.

5. Click Apply.
6. Repeat steps 3 - 5 if you want to create another group.
7. Click Close when you finish.
8. Add members to the group by right-clicking a user and selecting Properties. Or, right-click a user and select copy and then right-click the group and click Paste. The user is added to the new group.

Related topics

- [Using the Directory Utility](#)



Enabling users to create accounts



If you check the **Allow users to create accounts** checkbox on the Users/Groups window, you must provide an HTML file through which the accounts can be created. 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 as described below.

Accounts created in this way allow the new user to change password and save preferences.

When the HTML file is loaded, a Create User Account window appears. The user must fill in the information and click Apply to [create each account](#).

To customize `NewUser.html`:

1. Open the file in a text editor.
2. Change or add to the value for the Groups parameter as necessary; you can include multiple groups, separated by a comma. The value must be enclosed in double quotes.



If you are using LDAP, you cannot specify multiple groups.

3. Save the file with any name you choose.

You can create as many different files as you like, so that users can create accounts in different groups.

NewUser.html is similar to the following:

```
<APPLET archive=hodusd.jar
CODE="com.ibm.eNetwork.HODUtil.services.config.client.NewUser.class" WIDTH=454
HEIGHT=250>
<PARAM NAME=CABBASE VALUE=hodusd.cab>
<PARAM NAME="Groups" VALUE="HOD">
```

A customized file is similar to the following:

```
<APPLET archive=hodusd.jar
CODE="com.ibm.eNetwork.HODUtil.services.config.client.NewUser.class" WIDTH=454
HEIGHT=250>
<PARAM NAME=CABBASE VALUE=hodusd.cab>
<PARAM NAME="Groups" VALUE="HOD, Sales">
```



This function allows a user who knows the URL to create any number of user accounts, so you might want to control its use carefully.



Adding or modifying a user



To allow users to create accounts for themselves or for other users so they can use Host On-Demand sessions, select [Allow users to create accounts](#) on the Users/Groups window.


To modify a user, right-click the user and select Properties.

To add a user:

1. Click **Users/Groups** in the Administration window.
2. Click **New User** on the Users/Groups window.
3. Enter the required information.

User ID

Type the User ID. You can use only equivalent to English A-Z, a-z, 0-9, . (period), and - (hyphen). When using LDAP, User IDs can be mixed case. When using Host On-Demand to store configuration information, User IDs are converted to lowercase characters. IDs must be unique. You cannot have a user ID and a group ID that are the same, even if one is in lower case and the other is in upper.

 **Note for Windows users:** If you 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

Type a description of the user. You can use any character except | (vertical bar) and # (number or pound sign).

New Password

Type a password. You can use any character. A password is not required.

Confirm Password

Enter the password again.

4. Select one or more groups for the new user from the **Not a member of** list and click Add. A 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 that you want the user to be a member of.

5. If you do not want the user to be able to save preferences (changes that the user might make to a host session configuration), select **Do not save preferences**. This feature is useful for user IDs shared by more than one person.
6. If you do not want the user to change the password, select **User cannot change password**.
7. If you are using [native authentication](#), select **Use Native Authentication** and enter a user ID to be used for the authentication process.
8. Click **Apply**. Repeat the steps above to create another user account.
9. Click **Close** when you finish.

Related topics

- [Using the Directory Utility](#)

Deleting a user or group



1. Select Users/Groups in the Administration window.
2. Right-click the user or group you want to delete.
3. Select Delete.
4. If you are deleting a group and want to delete the user accounts of all the members of the group, click **Also delete all members of this group**.



This option is not available if you are using LDAP.

5. Click OK.

If you delete a group, the group's name is removed from the accounts of all the members of the group. If this is the last group, the users are automatically made members of the default group HOD, unless you check the Also delete all members of this group checkbox. Then all users are deleted instead of added to the default HOD group.



If you are using LDAP, you must delete the members and subgroups before you can delete the parent group.



Configuring a host session for a



user or group

1. Click Users/Groups in the Administration window.
2. Right-click the user or group and select Sessions.
3. Click the appropriate button in the Configure list. Fill in the necessary information. If you want to prevent the user from changing a field, click Lock.
4. Click OK. An icon for the session is added to the Configured Sessions window.
5. To make further changes, right-click the icon, then click Properties.
6. Click OK when you finish.
7. To change the session's runtime properties, such as keyboard mapping, colors, or macros, right-click the session and select Start Session. Make the changes as a user would customize his session. You can only change the session's runtime properties if you downloaded the Full administration client. For more information about the Full administration client, see [Administration clients](#).



Copying a user



You can copy users from one group to another using the copy and paste options.

1. Click Users/Groups in the Administration window.
2. Right-click a user or group.
3. Click Copy.
4. Right-click the group that you are adding the user to and click Paste User/Group. The user is added to the list of members for that group.



In LDAP mode, it is not possible to copy a user because a user can not be a member of more than one group.



Changing a user's or a group's



account

1. Click Users/Groups in the Administration window.
2. Select the user or group you want to change.
3. Right-click and select Properties.
4. Make the changes. For user account, you can change the two checkboxes as needed. If you want to change group membership, make the appropriate selections. You cannot change the ID.
5. Click OK.

Viewing a trace of a user's session

You can look at a trace file that has been created by a user and saved to the server. Trace files are saved in the `private` directory on the server as `SVRLOGANDTRACE.[user_name].user`.

1. Click Users/Groups on the Administration window.
2. Right-click a user and select Trace Facility.
3. You can copy the [trace information](#) into a text file so that you can study it or send it to IBM Service.



Changing the administrator user ID



and password

1. Click Users/Groups in the Administration window.
2. Right-click the Administrator ID from the User list and click Modify.
3. Type the new User ID (you can do this only for the administrator account).
4. Optionally, change the description.
5. Optionally, type a password and its confirmation.
6. Click OK.



Disabling graphical interface



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.



You cannot reduce download size by disabling functions. For more information about reducing download size, refer to [Preload Options](#).

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:
 1. Click Users/Groups.
 2. Right-click a group or user and select Disable Function.
- From the [Deployment Wizard](#):
 1. Define a host session.
 2. Click Disable Functions.

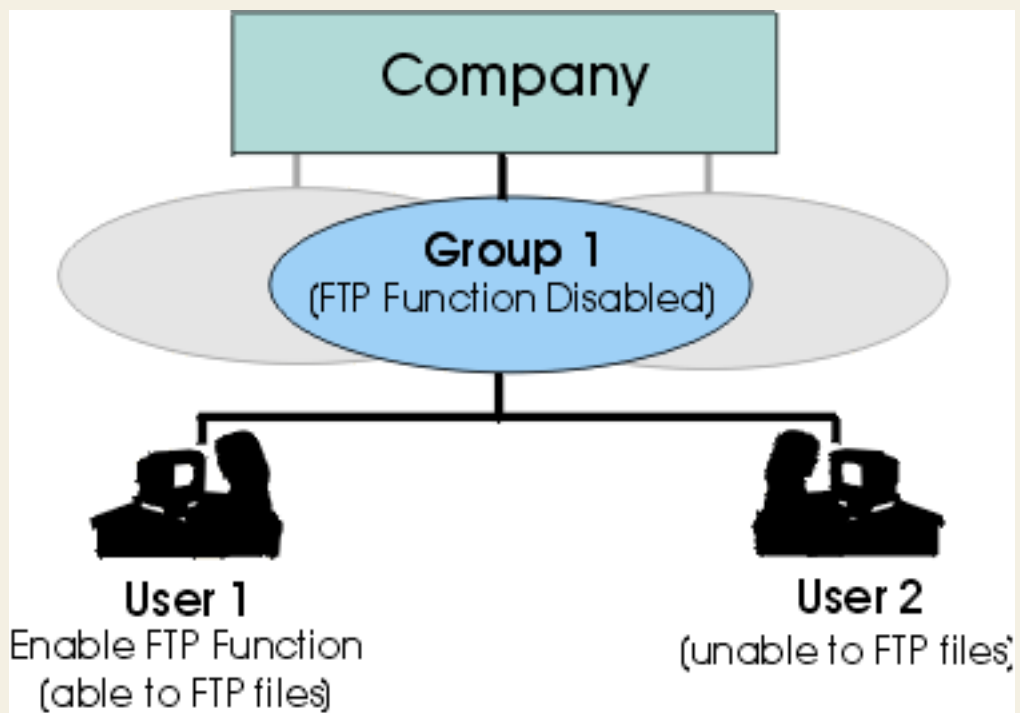
Changes made to a user's functions while the user is logged on do not become effective until the user has logged off and then logs back on.

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, 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. As depicted in the following figure, if at least one those groups has the function enabled, then the function is enabled for the user.



Related topic

- [Starting the Deployment Wizard](#)

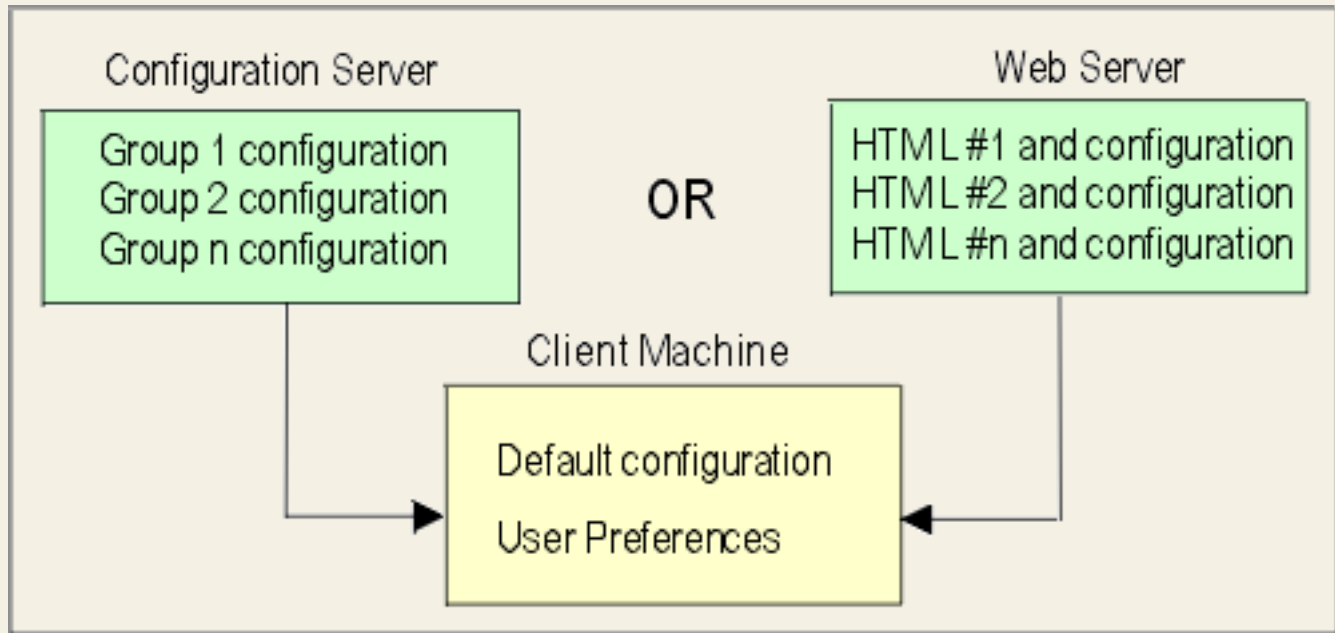
Creating your own user account

The administrator must provide an HTML file so that you can create an account for yourself.

1. Open a browser and type in the URL supplied by the the administrator to create a user account.
2. Type the User ID. You can use only A-Z, a-z, 0-9, . (period), and - (hyphen). User IDs are always converted to lowercase characters.
3. Optionally, type a description of the user. Any character is allowed except | (vertical bar) and # (number or pound sign).
4. Optionally, type a password and confirm it. Any character is allowed.
5. Click Apply.
6. Click OK when you finish.

Storing session configurations and user preferences locally

If you choose the [HTML-based model](#) or the [Combined model](#) in the Deployment Wizard, session configuration information and user preferences are stored locally on users' machines. If you use the HTML-based model, the session configuration information will initially be obtained from the HTML file. If you use the Combined model, the session configuration will initially be obtained from the configuration server.



Users are able to run sessions using the default configuration that you define. Users can modify this default configuration according to personal preference. These personalized changes are stored on users' local machines separate from any default session configuration information (assuming you gave them permission to save changes in the Deployment Wizard). When you change the default configuration, users will automatically receive updates without losing any personalized changes. If you [lock a particular session property](#), you will override any changes the user may have made to that particular property.

Where information is stored

The location where local preferences are stored is based on client platform, browser, browser JVM level, and Host On-Demand version. The chart below shows the location where Host On-Demand stores the local preferences based on these parameters.

Note: In certain cases, the location where local user preferences are stored has changed since the release of Host On-Demand V6.0. These changes in location are in response to the need to support the limited access rights of Windows Restricted Users. In cases where the locations have changed, if a user has existing preferences from a prior release of Host On-Demand, those preferences will be automatically migrated to the new location. The specific instances where the location of preferences has changed is noted in red in the chart below.

In the chart, the value *username* usually denotes the operating system userid currently logged on. However, with Netscape 4.x on Windows, it represents the Netscape profile id, which is not necessarily linked to the Windows login ID. The profile id has a default value called "default," although users can create their own profiles with Netscape's profile manager.

Platform and Browser	Host On-Demand Version 5	Host On-Demand Version 6	Host On-Demand Version 7
Windows 98 & IE			
Windows 98 & Netscape 4	\Windows\Java\HODData \Netscape\Users\username\HODData	\Windows\Java\username\HODData \Netscape\Users\username\HODData	\Windows\Java\username\HODData \Netscape\Users\username\HODData
Windows 98 & Netscape 6	\Windows\HODData	\Windows\username\HODData	\Windows\username\HODData
Windows 2000/XP & IE			
Windows 2000/XP & Netscape 4	\WINNT\Java\HODData \Netscape\Users\username\HODData \Documents&Settings\username\HODData	\WINNT\Java\username\HODData \Netscape\Users\username\HODData \Documents&Settings\username\HODData	\Documents&Settings\username\HODData \Netscape\Users\username\HODData \Documents&Settings\username\HODData
Windows 2000/XP & Netscape 6			
Windows NT & IE			
Windows NT & Netscape 4	\WINNT\HODData \Netscape\Users\username\HODData	\WINNT\username\HODData \Netscape\Users\username\HODData	\WINNT\Profiles\username\HODData \Netscape\Users\username\HODData
Windows NT & Netscape 6	\WINNT\Profiles\username\HODData	\WINNT\Profiles\username\HODData	\WINNT\Profiles\username\HODData
OS/2 and Netscape 4	\Netscape\Users\username\HODData	\Netscape\Users\username\HODData	\Netscape\Users\username\HODData
OS/2 and Netscape 6	\java13\JRE install dir\HODData	\java13\JRE install dir\HODData	\java13\JRE install dir\HODData
UNIX and Netscape 4	/home/username/.netscape/HODData	/home/username/.netscape/HODData	/home/username/.netscape/HODData
UNIX and Netscape 6	/home/username/HODData	/home/username/HODData	/home/username/HODData

Related topics

- [Deployment Wizard](#)
- [Deployment Wizard Connection Options](#)
- [Administration Utility](#)
- [Locking fields](#)

Using the Directory Utility

The Directory Utility is a command line Java application you can use to manage user, group or session configuration information stored either in Host On-Demand or in an LDAP server. The Directory Utility allows you to add or update large numbers of users, groups or sessions from an ASCII file, instead of individually through the Administration client. For example, you can use the Directory to:

- Add, update and delete groups
- Add, update, and delete users from groups
- Add, update and delete sessions from users or groups

The Directory Utility uses an ASCII file which defines the groups, users or sessions to be added, updated or removed. The text file needs to be in XML format, with a ".xml" extension.

[Running the Directory Utility](#)

[XML file format](#)

[XML file example](#)

Running the Directory Utility

On Windows NT and Windows 2000 the command or script file to run the Directory Utility and sample 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 text file are located in the *hostondemand\lib\samples\DirUtilCommandFiles* directory. The sample text file is called *Sample.xml*. The command or script files are called:

- DirUtil-AIX for AIX
- DirUtil-Novell.cnf for Novell
- DirUtil-OS2.cmd for OS/2
- DirUtil-UNIX for HP-UX, Linux, and Solaris
- DirUtil-AS400.sh for AS/400
- DirUtil-S390 for OS/390

To run the Directory Utility, type the following at the command line:

Note: The order of the parameters is important.

```
DirUtil-xxx filename.xml admin password [hostname] [port] [CON | FILE]
```

where:

- *DirUtil-xxx* is the Directory Utility command or script file for your operating system
- *filename.xml* is 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](#). 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* is the Host On-Demand Service Manager's hostname or IP address. This parameter is optional. The default hostname is localhost (127.0.0.1).
- *port* is the Host On-Demand Service Manager's port. This parameter is optional. The default Service Manager port is 8999.
- *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 filename is *myxmlfile.xml*, then your log file name is *myxmlfile.log*.



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.

For example, on AIX you could run:

```
DirUtil-AIX file.xml admin password myhostname 8999 CON
```

XML file format

The descriptions of the elements below describe the format for valid XML elements that can be included in the XML file the Directory Utility will use. A basic understanding of XML is assumed. Lines that begin with an "`<!--`" and end with "`-->`" are treated as comments. Elements are case sensitive.

To create or edit the XML file, you must use an ascii editor that generates valid unicode characters. If you receive the error **DIR0037 Fatal error: Invalid XML Character** while using the XML file with the Directory Utility, the ascii editor did not generate valid unicode characters. Use a different ascii editor that does generate valid unicode characters.

`<dirscript>`

`<action>`

`<group>`

`<groupid>`

`<description>`

`<parent>`

`<removeusers>`

`<user>`

`<userid>`

`<groupid>`

`<description>`

`<authentication>`

`<pw>`

`<nativeid>`

`<savepref>`

`<session>`

`<filename>`

`<groupid>`

`<userid>`

`<description>`

`<dirscript>..</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 the Directory Utility.

Attributes: none

Required elements: `<action type=xxx>`

Optional elements: none

<action type=xxx>..</action>

The action that is 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 the Directory Utility.

Attributes: "add", "delete" or "update"

Required elements: At least one of the following elements is required within the <action> element:

<group>..</group>

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>..</user>

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>..</session>

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, the same way that the Administration client adds a duplicate session.

<group>..</group>

The enclosing element for a group.

Attributes: none

Required elements:

<groupid>..</groupid>

A unicode text string that identifies the group in LDAP or Host On-Demand. 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.

Optional elements:

<description>..</description>

A unicode text string that describes the group. This element is only valid when the action type is "add" or "update".

<parent>..</parent>

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>..</removeusers>

This element allows you to delete all the users which belong only 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 which 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>..</user>

The enclosing element for a user.

Attributes: none

Required elements:

<userid>..</userid>

The user identifier. This element is always required. If you are using Host On-Demand the `userid` is converted to lower-case. If you are using LDAP the `userid` can be mixed-case.

`<groupid>..</groupid>`

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 LDAP and you specify multiple groups, an error message is generated and the user is not added. Groups specified must exist before you can add a user to them. If the action type is "update" the user is updated to have membership in this group.

Optional elements:

`<description>..</description>`

A unicode text string that describes the user.

`<authentication type=xxx>..</authentication>`

You can specify the authentication that is used for the user. Valid types are "native" and "pw". If this element is not specified, then no authentication will be configured for the user.

`<savepref>..</savepref>`

You can specify 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 is set for the user, so that the user is able to save preferences.

`<removegroupid>..</removegroupid>`

You can update a user so that they no longer have membership in the specified group. This element is only valid if the action type is "update". You must use a valid groupid which contains this user.

`<authentication type=xxx>..</authentication>`

The authentication used for the user. You can use either native authentication, only if you are also using LDAP, or password authentication. 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 LDAP.

Attributes: "pw" or "native"

Required elements:

`<nativeid>..</nativeid>`

The user ID of the user on the native operating system. This element is required and valid only when using LDAP and when the authentication type is "native".

Optional elements:

`<pw>..</pw>`

The password associated with the user. This element is only valid when the authentication type is "pw".

`<changepw>..</changepw>`

You can specify if the user is authorized to change their password. Valid values are Yes or No. If this element is not specified the default of Yes is set for the user, and the user is able 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>..</session>`

The enclosing element for a session.

Attributes: none

Required elements:

`<filename>..</filename>`

The file containing the session definition. You can create a session definition file by using the Export Session menu option from any defined Host On-Demand session. The default extension for session files is `.hod`. The `<filename>` element may contain the full path to the session file, and it is only required when adding a session.

`<description>..</description>`

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 in the <session> element:

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.

<userid>..</userid>

The user identifier for the user to which this session is being added. User ID's must already exist before the session can be added. You can include multiple <userid> elements to add this session for multiple users.

<groupid>..</groupid>

The group 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.

Optional elements: none

XML file example

Below is an example XML file that adds three groups, adds the users to the groups, and if the sessions are exported and the comments are removed, then adds the sessions to the users and the groups. On Windows NT and Windows 2000 the sample.xml sample file is located in the *hostondemand\lib\samples\DirUtil* directory. The sample.xml sample text file for the other operating systems is located in the *hostondemand\lib\samples\DirUtilCommandFiles* directory.

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Begin DTD - The DTD should not be modified.-->
<!DOCTYPE dirsript [
<!ELEMENT dirsript (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>
]>

<dirsript>
  <action type="add">
<!-- Add three groups -->
    <group>
      <groupid>3270GROUP</groupid>
      <description>Group with 3270 sessions</description>
    </group>
  </group>
```

```

        <groupid>5250GROUP</groupid>
        <description>Group with 5250 sessions</description>
    </group>
</group>
    <groupid>mygroup</groupid>
    <description>Group with parent</description>
    <!-- the parent element should only be specified if using
LDAP -->
    <!-- <parent>3270GROUP</parent> -->
</group>

<!-- Add a user to the 3270 group and give them a password. -->
<user>
    <userid>user1</userid>
    <description>First User</description>
    <authentication type="pw">
        <pw>mypw</pw>
        <changePW>yes</changePW>
    </authentication>
    <groupid>3270GROUP</groupid>
</user>

<!-- Add a user to the 5250 group and do not allow them to save their session
preferences -->
<user>
    <userid>user2</userid>
    <description>Second User</description>
    <authentication type="pw">
        <pw>mypw</pw>
        <changePW>yes</changePW>
    </authentication>
    <groupid>3270GROUP</groupid>
    <savepref>no</savepref>
</user>

<!-- The session elements are commented because the file may not exist. -->
<!-- If you would like to add a session, then export a session with the -->
<!-- correct file name and remove the comment tags before running DirUtil. -->

<!-- Add a session to the 3270 group -->
<!--
    <session>
        <description>3270 Display</description>
        <filename>3270dsp.hod</filename>
        <groupid>3270GROUP</groupid>
    </session>
-->

<!-- Add a session to the 5250 group -->
<!--
    <session>
        <description>5250 Display</description>
        <filename>5250dsp.hod</filename>
        <groupid>5250GROUP</groupid>
    </session>
-->

```

```
<!-- Add a session to user1 -->
<!--
    <session>
        <description>3270 Printer</description>
        <filename>3270prt.hod</filename>
        <userid>user1</userid>
    </session>
-->

    </action>
</dirscript>
```

The previous example added users, groups and sessions. To delete or update users, groups or sessions, change the action type to "delete" or "update" and make the appropriate changes to the elements.

Tracing on the client

To access the Trace Facility from a host session:

1. On the host session Actions menu, click Problem Determination.
2. Click Trace Facility.
3. Use the Log/Trace Facility online help for more information.

[Starting and stopping a trace](#)

[Saving a trace file](#)

[Viewing a trace file](#)

[Viewing a log file](#)

Starting and stopping a trace

1. Click Trace on the toolbar.
2. Select a [trace level](#) for each function and component. The function and the component are the source of the trace. The function is the name of the feature and the component is a specific part of the selected function. The higher the trace level, the more information that is traced.
3. Click Start.
4. Take the necessary steps to reproduce the problem.

The trace starts and captures trace and log messages. Messages are saved to a trace buffer. Once the default number of entries has been reached, trace entries start wrapping; new entries replace the old entries. To change the number of trace entries saved to the trace buffer, click [Settings](#).

To see trace messages as they are captured, click Console. However, running the console during a trace may affect performance.

5. Click Stop.

You can view the trace messages in the console or save it to a file (or both). To view the trace messages, click Console. To save the trace messages, click Save. To clear the current trace console and trace buffer, click Clear.

Saving a trace file

To save the log and trace information, click Save.

After running a trace and capturing data, choose where you want trace files to be saved by clicking Settings and then select Server or Local.

Server

If you select Server and Host On-Demand is downloaded from a Web server or installed as a local client, the file is saved on the server in the \private directory under the Host On-Demand installation directory.

The file is saved using the following naming convention:

SVRLOGANDTRACE.*username*.*user*

where *username* is the Host On-Demand user who is logged on and *user* is the file extension.

Local

If you select Local, name the file and choose where you want to save it.

Both

To save a trace file to both server and local:

1. Click Save.
2. Click Settings.
3. Select the other choice for Save Location and click OK.
4. Click Save.

Viewing a trace file

To view a previously saved trace file, open the file in a text editor.

To view the current trace file:

1. Click Trace on the toolbar.
2. Click Console. If the console is empty, then the trace buffer has been cleared.

Viewing a log file

1. Click Actions > Problem Determination.
2. Click View Log Messages.

To save log messages, copy and paste the information to a text file.

Log information contains messages about events that occur while the program is running. The events can be information, warnings, or errors. Log messages are always captured and are dynamically updated. When you view the log file, you see only log messages.

When you run the Trace Facility, log messages are also captured in the trace file. You can run a trace, save the captured messages to a file, and then view both log and trace messages in the console.



Welcome to the Host On-Demand Deployment Wizard

The Host On-Demand Deployment Wizard guides you through the necessary steps to create an HTML page that can be used to launch Host On-Demand host sessions. It provides a quick, easy interface to help you configure many available HTML features. Using the Deployment Wizard, you first select which [configuration model](#) that you want to use. For example, if you select the HTML-based model, you define all session information using the Deployment Wizard, and this session information is stored in the HTML file itself. If you select the Combined or Configuration Server-based models, you define your session information in the Host On-Demand Configuration Server using the [Administration Utility](#).

The following is a list of some of the many features that you can configure using the Deployment Wizard:

- **Preloads.** Host On-Demand runs as an applet and must download code to the users' machines. By default, the Host On-Demand client downloads all of the components, but you may reduce the download size by removing those components that are not needed. Refer to [Preload Options](#) for more information.
- **Download or cached client.** Download clients download the necessary applet files each time users access the HTML pages; cached clients retain the code the first time users access the HTML page, and will store it on the users' machines. Refer to [Selecting which clients to use](#) for more information.
- **Web page appearance (custom HTML templates).** You can easily set up a [template](#) that the Deployment Wizard will use to generate your HTML pages. This feature makes it easy to add your own background, banners, etc.
- **Client Java level.** Clients running [Java 2-enabled browsers](#) will need somewhat different HTML pages than those running Java 1-enabled browsers. In the Deployment Wizard, you can select Java 1, Java 2, or Auto-detect.
- **Cached client upgrade options.** When running the cached client, the code must be upgraded when newer versions of the client are available. There are a number of [Deployment Wizard options](#) that allow you to control when the upgrades occur.
- **Location of the Host On-Demand install (codebase).** Usually, Deployment Wizard files are placed in the Host On-Demand server's publish directory. However, sometimes it may be useful to put these files in a location that is independent of the Host On-Demand server so that they can be granted different security controls or make Host On-Demand server [upgrades](#) easier, for example.
- **Locale options.** The Host On-Demand applet will automatically display client desktop and session frame messages in the language identified by the locale on users' machines. However, using the [Advanced Options tab](#) on the Deployment Wizard, you can specify a particular locale to use if you wish to ignore the setting on each user's machine.
- **Portlets.** You can run Host On-Demand as [portlets](#) within the Portal Server component of WebSphere Portal. Administrators can use the Deployment Wizard to create custom Host On-Demand portlets with only the features they desire.
- **Windows Domain logon.** If your users are logged on to a Windows domain, this option automatically logs users on to Host On-Demand using their Windows user name. This is available with the Configuration Server-based model in the Deployment Wizard. Refer to [User ID Security](#) for more information.
- **Session Manager APIs.** The Host On-Demand Session Manager provides JavaScript APIs for managing host sessions and text-based interactions with host sessions. These APIs are intended to provide support for embedding host sessions into a Web page using JavaScript and can be enabled with the Deployment Wizard. Refer to the Host On-Demand Session Manager Reference for more information.

If you are configuring options (defining sessions) using the HTML-based model, you have an additional set of options:

- **Session properties.** All of the [session properties](#) can be configured, including connection information, security, etc. Each of the fields may be locked to prevent users from updating them.
- **Runtime options.** When configuring a session, you can start it and define runtime features such as session size and placement, colors, toolbar customization, and macros.

- **Disabling user functions.** You can [disable](#) almost any of the functions that users normally receive as part of their Host On-Demand session, such as bookmarking, creating or running macros, etc.

Related topics

- [Dynamically modifying session properties \(HTML overrides\)](#)
- [Using DWunzip to deploy Deployment Wizard files](#)

Configuring host sessions



Both administrators and client users can configure host sessions. Administrators can configure host sessions for groups or for users. Users can configure host sessions that have been provided to them by their administrator; however, the administrator can lock some or all of the fields.



Creating a session

1. On Windows NT, click Start > Programs > IBM Host On-Demand > Administration > Administration Utility. On other platforms, open HODAdmin.html in the HOD directory. You can open the Administrator window from any computer that has access to the Host On-Demand server.
2. Log on as the administrator.
3. Click Users/Groups.
4. Right-click the user or group for whom you want to create a session and select Sessions.
5. In the Configure box, click the display or printer session you want to create.
6. On each tab, type or select the required information.
7. Click OK.

Lock

Locking fields locks the startup values for a session. In most case, users can not change values for those fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Modifying a session configuration

1. Right-click the session's icon.
2. Click Properties.
3. On each tab, change the required information.
4. Click OK when you are finished.

To modify a session's runtime properties, such as remapping the keyboard, changing colors, or defining macros, the administrator can right-click on the session's icon, click Start Session, and make the changes in the session.

Modifying a session's runtime properties

In order to start a user or group session and change the session's runtime properties, such as keyboard mapping, color mapping, or macros, administrators must download one of the full administration clients:

- Full Administration client (HODAdminFull.html)
- Full Administration client cached (HODAdminCachedFull.html)
- Full administration client cached with problem determination (HODAdminCachedDebugFull.html)

Full administration clients have all the capabilities of Host On-Demand administration clients. To make runtime changes, the administrator right-clicks on the session and selects Start Session. The session starts, and the administrator can make the changes just as the user would. Note the following limitations of the full administration client:

- You cannot change the runtime properties for a multiple session icon. You need to update each session individually.
- You can only update the runtime properties of a session if you have specified that the session should launch in a

separate window. To check this, right-click on the session's icon, select Properties, click on the Advanced tab, and make sure the Start in Separate Window radio button is set to Yes.

- You can only update one session at a time. When you start a user or group session, the other Host On-Demand windows are disabled. Save the session and close it to enable the other Host On-Demand windows again.
- The full administration clients download more files than the other administration clients. If you don't plan to change the session's runtime properties, you can save space by downloading the other administration clients instead. If you have the regular administration client installed and you try to change the session's runtime properties, you are prompted to install one of the full administration clients.

Copying a session

1. Right-click the session icon that you want to copy.
2. Click Copy from the menu.

The session is copied to the clipboard for the Administration utility. You can now paste the session to another user's or group's configuration.

If you copy a session configured for multiple sessions, you must individually copy all of the sessions contained within that configuration. For example, if the multiple session icon is configured to start a 3270, a 5250, and a 3270 print session, you need to copy each of those three sessions and the multiple session icon.

Pasting a session

You cannot paste a session until you have copied a session to the clipboard. There are two ways you can paste a new session. If you plan to make updates to each new session, pasting to the Configured Sessions window enables this more quickly. If your goal is to add new sessions quickly to many users and groups without changing session properties, pasting to the Users/Groups window enables this more quickly.

Pasting to the Configured Sessions window

1. Right-click the user or group into which you want to paste the session currently on the clipboard.
2. Click Sessions from the menu.
3. Right-click in an empty area of the Configured Sessions window.
4. Click Paste from the menu.

You see the new session icon pasted into the Configured Sessions window with the same configuration as the original session you copied. If the new user or group already has an existing icon with the copied session name, a number is added to the beginning of the new icon's name to indicate it is a copied session. For example, if the original session name is **3270 Session**, the name of the copied session is **1:3270 Session**.

5. To make any changes, such as the session name, right-click the new icon and click Properties.
6. To make another copy, right-click in an empty area of the Configured Sessions window and click Paste. Repeat for as many copies as you want.

If you paste a session configured for multiple sessions, you must individually copy and paste all of the sessions contained within that configuration. For example, if the multiple session icon is configured to start a 3270, a 5250, and a 3270 print session, you need to copy and paste each of those three sessions and the multiple session icon.

If you paste a session with associated printers defined, you need to open the session's properties (right-click the icon and click Properties) to verify that the associated printer settings are correct. Save the session when the associated printer settings are defined correctly.

Pasting to the Users/Groups window

1. Right-click the user or group into which you want to paste the session currently on the clipboard.
2. Click Paste Session.

The new session is pasted into the selected user or group with the same configuration as the original session you copied. You will need to open the Configured Sessions window for that user or group to make any changes to the new session, such as the session name. If the new user or group already has an existing icon with the copied session name, a number is added to the beginning of the new icon's name to indicate it is a copied session. For example, if the original session name is **3270 Session**, the name of the copied session is **1:3270 Session**.

3. To make any changes, such as the session name, open the Configured Session window for the new user or group, right-click the new icon, and click Properties.
4. To make another copy, in the Users/Groups window right-click the user or group to which you want to add the new session and click Paste Session. Repeat for as many copies as you want.

If you paste a session configured for multiple sessions, you must individually copy and paste all of the sessions contained within that configuration. For example, if the multiple session icon is configured to start a 3270, a 5250, and a 3270 print session, you need to copy and paste each of those three sessions and the multiple session icon.

If you paste a session with associated printers defined, you need to open the session's properties (from the Configured Sessions window, right-click the icon and click Properties) to verify that the associated printer settings are correct. Save the session when the associated printer settings are defined correctly.

Duplicating a session

1. Right-click the session's icon and click Duplicate Session.
A new icon appears in the Configured Sessions window with a number added to the beginning to indicate it is a duplicated session. For example, if the original session name is **3270 Session**, the name of the first duplicated session is **1:3270 Session**. The new session has the same configuration as the original session you duplicated.
2. Right-click the new icon and click Properties to make any changes, such as the session name.
3. To make another duplicate, right-click the session's icon, either the original or the copied session icon, and click Duplicate Session again.

Related topics

- [Copying a session for the client](#)
- [Configuring a session for easy launch](#)
- [Deleting a session](#)

Configuring clients to use client authentication

Client authentication can be configured in the session configuration properties on the server or on the client workstation.

On the server:

1. Open the Administrator window.
2. Click the Users tab to open the list of defined groups and users
3. Select a user or group and click Sessions to open the Configured Sessions window.
4. If you are creating a new session, click the appropriate button. If you are changing a session, right-click the session icon, then click Properties.
5. Click the [Security tab](#) and then click Enable Security.
6. To enable server authentication, click [Server authentication](#). Read about known [security limitations](#) when using the Internet.
7. To use [client authentication](#), click Yes for Send a Certificate.
8. Then specify the [Certificate Source](#) and [Certificate Location](#) or [Certificate Name](#).

To specify a default location of the client certificate, enter a URL or path and file name. The URL protocols that can be used depends on the capabilities of your browser. Most browsers support http, https, ftp, and ftps.

To specify a default name, choosing "Any certificate trusted by the server" causes Host On-Demand to search through the Microsoft Internet Explorer Personal Certificate store for the first certificate that is signed by a Certificate Authority trusted by the server requesting the certificate. Choosing a specific name causes Host On-Demand to send only that certificate. You may also add the name of a certificate that is not in the administrator's Certificate Store by clicking the "Add Certificate Name" button and specifying certificate components, such as the common name, organization, etc.

Note: If you do not want the location or name changed, click Lock. Otherwise, users can choose the certificate location or name.

To be prompted each time the server requests a client certificate, click "Prompt on each connection" for [How Often to Prompt](#). To be prompted once each time you start Host On-Demand, click "Prompt the first time after HOD is started".

Specify whether or not to [Retrieve Certificate before Connecting](#).

9. Click OK.
10. If clients will use secure sessions to the Host On-Demand server, click the Redirector service.
 - If you are creating a new redirector connection, click Add. If you are changing a connection, highlight the entry and click Change.
 - In the Add (or Change) Configuration window, choose the appropriate value for Security. The most likely choice is Client-side because this provides secure sessions between the client and the Redirector. Refer to the online help for more information.

On the client:

Note: Some of the following fields may have been disabled by the administrator.

1. If you want to create a new session, click Add Sessions and double-click the type of session you want to create. If you want to change an existing session, right-click the session icon, then click Properties.
2. Click the [Security tab](#) and then click Enable Security.

3. To enable server authentication, click [Server authentication](#). Read about known [security limitations](#) when using the Internet.
4. To use [client authentication](#), click Yes for Send a Certificate.
5. Then specify the [Certificate Source](#) and [Certificate Location](#) or [Certificate Name](#).

To specify a default location of the client certificate, enter a URL or path and file name. The URL protocols that can be used depends on the capabilities of your browser. Most browsers support HTTP, HTTPS, FTP, and FTPS.

To specify a default name, make a selection from the Certificate Name drop-down box. Choosing "Any certificate trusted by the server" causes Host On-Demand to search through the Microsoft Internet Explorer Personal Certificate store for the first certificate that is signed by a Certificate Authority trusted by the server requesting the certificate. Choosing a specific name causes Host On-Demand to send only that certificate.

To be prompted each time the server requests a client certificate, click "Prompt on each connection" for [How Often to Prompt](#). To be prompted once each time you start Host On-Demand, click "Prompt the first time after Host On-Demand is started." If your client supports [storing preferences locally](#), choosing "Prompt only once, storing preferences on the client" causes Host On-Demand to prompt the next time the connection is made, but never after that, unless the connection is attempt fails.

Specify whether or not to [Retrieve Certificate before Connecting](#).

6. Click OK.

Not all servers request certificates. When you try to connect to a telnet server that does, a window appears prompting you for the location and password of your certificate.



Setting security on the Redirector

To use secure sessions on a Host On-Demand Redirector, you must set a security level on the port used by the Redirector. On the server:

1. Log on as the administrator.
2. Click the Redirector tab.
3. If you are creating a new connection, click Add. If you are changing a connection, highlight the entry and click Change.
4. In the Add (or Change) Configuration window, choose the appropriate value for Security. The most likely choice is Client-side because this provides secure sessions between the client and the server. Refer to the online help for more information.

Related topics

- [How TLS and SSL work](#)
- [Server authentication](#)
- [Client authentication](#)

Remapping the keyboard



[Key assignment](#)

[Assigning keys to functions](#)

[Assigning keys to custom functions](#)

[Assigning keys to applets](#)

[Assigning keys to macros](#)

[Unassigning keys](#)

[Searching for key assignments](#)

[Restoring key assignments](#)

[Restrictions for key remapping](#)

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.

Key Assignment

Category

Select the category of function you want to work with, for example, Characters, Host Functions, Custom Functions, and Menu Commands.

When you select a category, the specific functions within that category appear in the table below, along with the keys assigned to those functions. Select a function in this table to change its key assignment. Refer to [Default Characters and Functions](#) for more information.



Note that if the administrator has disabled Edit Keyboard Mappings, the only available button on this screen will be Search for Key.

Assign a Key

After selecting a function, click this button to assign a key to it.

Unassign Key

After selecting a function, click this button to undo its key assignment.

Custom Functions

Click this button to bring up the [Custom Function Editor](#). Certain keyboard functions are predefined with Host On-Demand for remapping. The Custom Function Editor allows you to define and maintain new keyboard functions, called custom functions, without having to edit HTML and Java script files. These new functions may be mapped to key combinations, much like the predefined keyboard functions. Using the Custom Function Editor, you can add or delete a custom function. You can then go to the Keyboard Remap dialog, choose Custom Functions from the Category list, and your defined custom functions will appear in the list available for remapping. You can also assign a toolbar button to a custom function from the Keystroke page of the Customize Toolbar dialog.

Reset Key

Click this button and then select a key to restore the key to its default assignment.

Reset All

Click this button to restore the default key assignments to all functions.

Search for Key

Click this button to find out if a certain key has already been assigned to a function. If there is a function already assigned to this key, that function will appear highlighted along with its assigned key.

Assigning keys to functions

To assign or reassign a key to a function:

1. Start from a host session window.
2. Click Edit > Preference > Keyboard, or click the Remap button on the toolbar.
3. Click the Key Assignment tab.
4. Select a Category.
5. Select the function you want to assign a key to.
6. Click Assign a Key.
7. On your keyboard, press the key you want to assign to this function.



You can assign a key combination to a function using the Alt, Ctrl, and Shift keys (for example, Alt+F1 or Ctrl+Alt+Q). If your browser is a version of Netscape earlier than 6.x, you might experience problems attempting to assign a key combination to a function using the Alt key. If this happens, you should not use Alt in key combinations.



If the key has already been assigned to a function, you will be shown the function that that key is assigned to and told to unassign the key first.

8. After you have successfully assigned all the keys you want, click OK.

Assigning keys to custom functions

If you want to assign a key or key combination to a custom function that is not currently listed in Keyboard Remap under the Custom Functions category, you can define these functions using the [Custom Function Editor](#). When you do this, the Custom Functions category will appear with your newly defined functions, which can then be assigned to any key. Complete the assignment by following the steps for [Assigning keys to functions](#), choosing Custom Functions as the category.

You can optionally define a custom function in the HTML or Java script file used to start the sessions. See [adding additional HTML parameters](#) for more information.

Assigning keys to applets

To assign or reassign a key to an applet, you must first run the applet:

1. Start from a host session window.
2. Click Actions > Run Applet, or click the Run Applet button on the toolbar.
3. Type the name of the applet you want to run, and click Run.

The applet is now available for a key assignment.

4. Complete the assignment by following the steps for [Assigning keys to functions](#).

Assigning keys to macros

1. Before you can assign a key combination to a macro, you must create a macro, either by clicking Actions > Record Macro *or* by importing a macro using the [Macro Editor](#).
2. Click on Edit > Preferences > Keyboard to access the Key Remapping facility.
3. Use the pull-down menu to select the Macro category. (If the Macro category does not appear, cancel out of the Key Remapping facility and wait a few moments for the Key Remapping facility to be notified of the macro change.)
4. Once you have selected the Macro category, your macro should appear in the list in the table, and you can assign a key combination to it by following the steps for [Assigning keys to functions](#).

Unassigning keys

To undo an assignment of a key to a function, select the function, and then click Unassign Key.

Searching for key assignments

To find out if a key has already been assigned to a function:

1. Click Search for Key.
2. On your keyboard, press the key or key combination you are interested in.

If there is that key has already been assigned a function, that function will appear highlighted along with its assigned key. If no function is assigned to that key, a "Not Assigned" message will appear.

Restoring key assignments

To restore a previously reassigned key to its default assignment:

1. Click Reset Key.
2. Click the key you want to restore.

To restore all keys to their default assignments, click Reset All.

Key assignments are saved automatically if you are an administrator or a defined user.



The Ctrl key is mapped to the Enter function by default for the 3270 and 5250 emulators. Because Java does not distinguish between left and right Ctrl keys, this change means that both Ctrl keys now act as Enter. You can still remap Ctrl or use it in combination with another key, and you can still remap the Enter function to any other key.

Restrictions for key remapping

Restrictions for key remapping include the following:

- When using Java 2 with Host On-Demand, the Ctrl-Tab key and the Ctrl-Shift-Tab key combinations cannot be remapped. With Java 2, these key combinations are consumed by the Java Focus Manager and are not returned to Host On-Demand for processing.
- In Host On-Demand, certain key combinations are treated in a similar fashion and cannot be assigned to different keyboard functions.

JVM key events, such as key pressed and key released, are dependent upon the operating system and keyboard

layout of the machine where they are processed. The JVM makes no distinction between the following:

- a key function for Enter received from the main Enter key or the keypad Enter key
- a key function for Control received from the right or left Control keys
- a key function for Alt received from the right or left Alt keys

If the JVM receives a key function for Enter from either the main Enter key or the keypad Enter key, the key stroke will be processed as an Enter key event. To the JVM, the two key strokes are not distinct. Similar processing will occur for the Control and Alt key functions defined in the same manner.



Note that on some operating systems, these sets of keys are defined differently. On AIX, the right Control key is defined with the Execute key function, not the Control key function. In this case, the JVM will treat the key strokes from the right and left Control keys differently.

Because of these JVM limitations, Host On-Demand is also unable to distinguish between two keys defined in the manner stated previously. A Host On-Demand user or administrator cannot assign different key remapping functions to

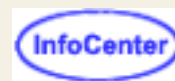
- the same key combination using the main Enter key and the keypad Enter key,
- the same key combination using the right and left Control keys, or
- the same key combination using right and left Alt keys

if the JVM processes these keys as the same key event. For example, if Right Ctrl+P is processed the same as Left Ctrl+P by the JVM, then these key combinations cannot be assigned to different key remapping functions in Host On-Demand.

Related topics:

- [Specifying a key as repeating or non-repeating](#)
- [Default characters and functions](#)

Session parameters



- [Session1 parameters](#)
- [Session2 parameters](#)
- [Saving preferences parameters](#)
- [3270 and 5250 host print session parameters](#)
- [3270 host print session only parameters](#)
- [5250 host print session only parameters](#)
- [Disabling functions](#)
- [Cached client installation parameters](#)

Session1 parameters

Parameter name	Description	Valid values	Default value
User	User ID	The ID of the user.	None
Password	Password	The user's password.	None
Launch	The name of the session as typed in the configuration panel. The case of the characters must match exactly (upper/lower). If the name includes one or more spaces, you must enclose it in double quotes (" ").	The name of the session	None
Embedded	Run the session embedded in an HTML file or in a separate window.	true = Run embedded within the browser file false = Run in a separate window	false
Locale	Sets the locale.	xx_YY xx = language code YY = country or region code	Locale returned by the JVM

Session2 parameters

Parameter Name

Description	Valid values	Default value	
SessionName	The name you want to assign to this session (appears at the top of the window).	Any string	None
MaxSessions	Limits the number of sessions a user can start.	Integer	None
Host	Host name or IP address of the target telnet server.	Host name or IP address	None

WorkstationID	Name of this workstation.	Unique name for this workstation	None
SessionType	The type of session you want to configure.	1 = 3270 2 = 5250 3 = VT 4 = CICS gateway 5 = 3270 printer 6 = 5250 printer	1
SessionID	The short name you want to assign to this session (appears in the OIA). It must be unique to this configuration.	One character	A
GUIEmulation	Session uses Screen Customizer. When true, the Embedded parameter is ignored and the session is run in a frame.	true, false	false
ButtonText	Text on the start session button.	text string	Start Session or Start Session: <i>SessionName</i>
Port	The port number on which the target telnet server is listening.	Any valid TCP/IP port number	23 (CICS 2006)
TNEnhanced (3270 only)	Enable TN3270E support.	true, false	true
SLPEnabled	Enable SLP support.	true, false	false
SLPAS400Name	SLP AS400 Name	String - 8 + 8 with "." as a delimiter Net ID "." LU Name. Fully qualified CP name: 1-8 byte character string for each Net ID, and LU Name. The first character must be alphabetic(A-Z) or a special character (@,#,\$). The remaining characters can be alphanumeric (A-Z, 0-9) or special characters(@, #, \$).	""
SLPScope	SLP Scope	String - alphanumeric or special characters which include comma, asterisk, equal sign, plus sign, colon, semicolon, quotation marks, vertical bar, question mark, slash, backslash, left angle bracket (<), right angle bracket, left square bracket ([), right square bracket and the number sign (#).	*
SLPThisScopeOnly	SLP this scope only.	true, false	false
SLPMaxWaitTime	SLP maximum wait time.	integer	200

LUName	The name of the LU or LU Pool, defined at the target server, to which you want this session to connect. If you do not specify this, the session connects to the first available LU.	The name of an LU or LU Pool	None
ScreenSize	The number of rows and columns on the screen.	2 = 24x80 3 = 32x80 (3270 only) 4 = 43x80 (3270 only) 5 = 27x132 (3270, 5250 only) 6 = 24x132 (VT only)	2
CodePage	The code-page of the zSeries or iSeries to which the session will connect.	A supported host code-page	037
Locale	Sets the locale.	xx_YY xx = language code YY = country or region code	Locale returned by the JVM
DBCSInputVisible	DBCS input visible.	true, false	false
SSL	Enable SSL encryption.	true, false	false
SSLServerAuthentication	Enable server authentication by SSL.	true, false	false
AutoConnect	The session connects automatically when it starts.	true, false	true
AutoReconnect	The session re-connects automatically if the link recovers after failure.	true, false	true
StartupApplet	The name of an applet to start when the session starts.	The name of the applet's class file	None
OIAVisible	Show or hide the OIA (operator information area) in the session window.	true = On false = Off	true

Keypad	Show or hide the keypad in the session window.	true = Show the keypad false = Do not show the keypad	false
Toolbar	Show or hide the toolbar in the session window.	true = Show the toolbar false = Do not show the toolbar	true
ToolbarText	Show text that explains the purpose of each toolbar button.	true = Show the text false = Do not show the text	true
Statusbar	Show or hide the status bar at the bottom of the session window.	true = Show the status bar false = Do not show the status bar	true
VTTerminalType (VT only)	The terminal-type required by the server to which the session will connect.	1 = VT220_7_BIT 2 = VT220_8_BIT 3 = VT100 4 = VT52	1
VTNewLine (VT only)	New-line operation	true = CR false = CRLF	true
VTBackspace (VT only)	Backspace mode	true = Delete false = Backspace	false
VTLocalEcho (VT only)	Local-echo mode	true = On false = Off	false
VTCursor (VT only)	Cursor mode	true = Application false = Normal	false
VTKeypad (VT only)	Keypad mode	true = Application false = Normal	false
VTAutowrap (VT only)	Auto-wrap	true = On false = Off	false
CICSServerName (CICS only)	The host name or IP address of the CICS Gateway for Java.	Host name or IP Address	None
CICSGWCodePage (CICS only)	The code-page defined at the CICS gateway.	A supported CICS-Gateway code-page	000 (auto-detect)
LightPenMode	Light pen support	true = On false = Off	false
Embedded	Run the session embedded in an HTML file or in a separate window.	true = Run embedded within the browser window false = Run in a separate window	false
MacroManager	Show the Macro Manager toolbar.	true=Yes false=No	false

TraceLevel	Trace level	0 = Off 1 = Minimum 2 = Normal 3 = Maximum	0 = Off
FontName	Font name	font name	monospaced
FontStyle	Font style	0 = Plain 1 = Bold 2 = Italic	0 = Plain
FontSize	Font size	integer	12
Rule	Displays rule lines on the screen.	true, false	false
BlockCursor	Changes the cursor to a blinking solid block.	true, false	false
markedAreaPrintingEnabled	Enables print screen only for the marked area.	true, false	true
SESSION_QUIETMODE	Allows users to start a 3270 session without beeping noises.	true, false	false
3270InputAreaIndication	Indicates unprotected fields using dots ("."), underlines, or 3D rectangles.	1=Underdot,Underline,3D 2=Display,NonDisplay,DisplayAndNonDisplay Display - unprotected displayable fields are indicated NonDisplay - unprotected nondisplayable fields are indicated DisplayAndNonDisplay - all unprotected fields are indicated	None
NumeralShape (BIDI only)	Numeral Shape	NOMINAL NATIONAL CONTEXTUAL	NOMINAL
TextType (BIDI only)	Text type	VISUAL, LOGICAL	VISUAL
TextOrientation (BIDI only)	Text Orientation	LEFTTORIGHT RIGHTTOLEFT	LEFTTORIGHT
ThaiDisplayMode (Thai only)	Thai display mode	1 = Non-composed 2 = Composed 3 = Composed with space alignment 4 = Composed with EOF alignment 5 = Composed with space and EOF alignment	5

Saving preferences parameters

You can save all the configuration information to a single configuration file and then use that configuration file to configure the session when a downloaded client starts the session.

Note: Microsoft Internet Explorer and Netscape Navigator write the session preferences file to a different directory on the client system. Preferences saved using one of the browsers will not be loaded by the other.

Parameter name

Description	Valid values	Default value
Save	Name of a local file in which preferences must be saved.	filename

Config	The name of a file on the server from which preferences must be read. You cannot save changes here. The file can be either an absolute URL or a relative file name to the Session2.html document URL.	filename	
ConfigDefault	True: first time reads from the server, saves locally. After the first time, reads from local file. False: reads from server and local files, and combines. When both the Save and Config parameters are specified, the ConfigDefault parameter is used. When set to true (the default) the config file on the server will only be read if the config file on the local hard drive is not found. If set to false both the config file on the server and on the local hard drive will be read and combined into a single configuration object.	true, false	true
ConfigOverwrite	True: Reads from server and local files; if conflict, server definitions prevail. Additions saved locally. False: Reads from server and local files; if conflict, local definitions prevail. Changes or additions saved locally. When both the Save and Config parameters are specified and the ConfigDefault parameter is set to false, the ConfigOverWrite parameter is used. When both config files are read and combined into one configuration object, collisions with data will occur. This parameter controls the outcome of those collisions. If set to true, information in the server config file will be used in the case of a collision. If set to false (the default), information in the local config file will be used in the case of a collision.	true, false	false

3270 and 5250 host print session parameters

Parameter name	Description	Valid values	Default value
useWindowsPrinter	Choose whether Windows printer (either in GDI or Windows spooler mode) is used or not.	true, false	true on Windows platforms, false on other platforms
useWindowsDefaultPrinter	Choose whether Windows default printer is used or not.	true, false	true
windowsPrinterName	Windows printer name to be used for printing.	string	none
printDestination	Choose whether the output should go to a printer or to a file. When true, it goes to printer.	true, false	true
printerName	The name of the port for the printer to be used.	Any valid printer names	LPT1
printFileName	The path and name of the file when the print destination is a file.	Any valid path name	none
separateFiles	When the print destination is a file, choose whether you want to save each print job to a unique file or have jobs appended to each other in one file.	true, false	false
intervTime	The amount of time in seconds to wait for printing to start. If printing does not start within the time set, an Intervention Required message pops up.	Integer between 10 and 255	25
graphicsVisible	Display a window that includes several items of information, and shows the printer, workstation and host system as icons.	true, false	true

3270 host print session only parameters

Parameter name	Description	Valid values	Default value
usePDT	Choose whether PDT mode printing is used with a Windows printer.	true, false	false
faceName	Font name to be used for Windows non-PDT printing	string	Varies on the system locale. With US English, it is Courier New.
bestFit	Choose whether selected CPI/LPI will override the commands sent by the host. It will work correctly only when the host does not send the command to set CPI/LPI/MPP/MPL.	true, false	false
printBufferSize	The size of the block of memory reserved for print data that is being sent to the printer. This applies only to LU3 sessions.	1920, 2560, 3440, 3564	1920
PDTFile	PDT resource path name with directory name from the code base directory where HOD is installed.	Full path string to a PDT file	/pdfpdt/basic.hodpdt
charsPerInch	The number of characters printed per inch	Entries defined in the PDT	Taken from the DEFAULT_CPI? entry in the PDT if this entry exists.
linesPerInch	The number of lines per inch.	Entries defined in the PDT	Taken from the DEFAULT_LPI? entry in the PDT if this entry exists.
maxLinesPerPage	The maximum number of lines per page, including the top and bottom margins.	Integer between 1 and 255	Taken from the MAXIMUM_PAGE_LENGTH entry in the PDT. If the entry is not found, the default value, 66, is used.
maxCharsPerLine	The maximum number of characters per line.	Integer between 1 and 255	Taken from the MAXIMUM_PRINT_POSITION entry in the PDT. If the entry is not found, the default value, 132, is used.
suppressNullLines	Suppress the lines that contain only non-printable characters. This parameter applies only to an unformatted LU Type 3 job and when bits 2 and 3 in the Write Control Character (WCC) are not B'00'.	true, false	Taken from the COMPRESS_LINE_SPACING? entry in the PDT. If the entry is not found, the default value, false, is used.
printNullsAsSpaces	Print Nulls as spaces (X'40'). This parameter applies only to LU Type 3 sessions.	true, false	Taken from the OVERRIDE_FORMATTED_PRINT? entry in the PDT. If the entry is not found, the default value, true, is used.
suppressAutoNewlineCR	Suppress an automatic-new-line if there is a Carriage Return (CR) code at (Maximum Print Position) MPP+1. This parameter applies only to an unformatted LU Type 3 job and when bits 2 and 3 in the Write Control Character (WCC) are B'00'.	true, false	Taken from the NO_AUTO_NL_IF_CR_AT_MPP_PLUS_1? entry in the PDT. If the entry is not found, the default value, false, is used.

suppressAutoNewlineNL	Suppress an automatic-new-line if there is a new-line (NL) code at MPP+1. This parameter applies only to an unformatted LU Type 3 job and when bits 2 and 3 in the Write Control Character (WCC) are B'00'.	true, false	Taken from the NO_AUTO_NL_IF_NL_AT_MPP_PLUS_1? entry in the PDT. If the entry is not found, the default value, false, is used.
ignoreFFFfirstPos	If the session is LU Type 3 and you choose true, a form feed (FF) at the first position on the first line is ignored. If the session is LU Type 1 and you choose true, an FF or a CR+FF combination at the beginning of a print job is ignored.	true, false	Taken from the IGNORE_FORM_FEED_AT_FIRST_POS? entry in the PDT. If the entry is not found, the default value, false, is used.
FFtakesPrintPos	If you choose true, FF is executed, takes a print position and is printed as a blank in the first position on the first line of the next page. Therefore, the next print-position will be the second position of that line. If you choose false, FF is executed and the next print-position is the first position on the first line of the next page. That is, FF does not take a print position. This parameter applies only to LU Type 3 sessions.	true, false	Taken from the FORM_FEED_TAKES_POSITION? entry in the PDT. If the entry is not found, the default value, false, is used
formFeedPosition	If you choose true, FF is performed wherever it appears. If you choose false, FF is performed only if it appears at column 1. When FF is not at column 1, it is printed as a space character. This parameter applies only to LU Type 3 sessions.	true, false	Taken from the FORM_FEED_ANY_POSITION? entry in the PDT. If this is defined as Any, true is used. If the entry is not found, the default value, false, is used.
ignoreAttr	Choose true to ignore all 3270 attributes except non-printable attributes. This parameter applies only to LU Type 3 sessions.	true, false	false
drawFieldAttr	Use this parameter to determine how the 3270 field-attribute byte is drawn. If you choose 0 (None), the field-attribute byte is drawn as a space character without an attribute. If you choose 1 (Here), the field-attribute byte is used to draw the current byte. For example, if the current byte is defined as an underscore field, the field-attribute byte is drawn as a space character with the underscore attribute. If you choose 2 (Next), the field-attribute byte is used to draw the next field-attribute byte. This parameter applies only to LU Type 3 sessions.	0, 1, 2	0

concatTime	The expiration time for the print-job concatenation timer, which starts at the end of a print job. If the next print job arrives before the timer expires, that job is treated as a continuation of the previous job. If the time expires, an end-of-job command is sent to the printer and the next job is treated as a separate job. The value is specified in seconds.	Integer	0
termTime	The expiration time for the print-job termination timer, which starts at the end of the print data. If another print-data record arrives before the timer expires, that job is treated as the continuation of the previous record. Otherwise, an end-of-job command is sent to the printer and the next print record is treated as the beginning of a separate print job.	Integer	0
SCSSense	If you choose true, a negative response is sent to the host when an incorrect SCS command or parameter is received. If there is more data in the job, printing continues, though some of the printed data may be incorrect. If you choose false, printing continues but no notification is sent to the host. If there is a physical printer or connection problem, a sense-code is sent to the host even if you choose false. This parameter applies only to LU Type 1 sessions.	true, false	true
inheritParms	If you choose true, the parameters used in LU Type 1 print-job processing, such as tab positions, MPP or MPL, are inherited by the next job. This parameter is used when the host system sends a formatting command such as Set Horizontal Format for the first job, but assumes that the second and later jobs will use the format that is set for the first job. This parameter applies only to LU Type 1 sessions.	true, false	false
tractor	If you choose true, a form feed is not sent at the page boundary; a newline (NL) is sent instead. However, if a SET_AUTO_PERFORATION_SKIP command is defined in the PDT, a form feed is not sent, regardless of the setting of this parameter.	true, false	false

printerFontCodePage	This parameter is useful only for printers that do not support the default code page. It defines the ASCII code-page used for the printer (hardware) font. It should be consistent with the character code-points specified in the PDT file.	Integer	850 for Latin-1 countries or regions and the respective country or region's default ASCII code-page for other countries or regions.
pa1KeyVisible	Choose whether to have a button on the screen for the Program Attention 1 key. The function of the key depends on the host application.	true, false	false
pa2KeyVisible	Choose whether to have a button on the screen for the Program Attention 2 key. The function of the key depends on the host application.	true, false	false
PDTFile	PDT resource path name with directory name from the code base directory where HOD is installed.	Full path string to a PDT file	/pdfpdt/basic.hodpdt
TermAssocPrinter	This parameter closes the associated printer session when the 3270 display session is closed. This parameter takes effect for all 3270 sessions defined for that user. The user must close the 3270 session. Disconnecting the session has no effect. Default behavior stays the same.	true, false	true

5250 host print session only parameters

Parameter name

Description	Valid values	Default value	
messageQueue	The name of the queue where operational messages for the printer device are sent.	String	QSYSOPR
messageLibrary	The name of the library where the printer message queue is located.	String	*LIBL
hostFont	The font ID used for a print file if a font is not specified by the application. See session configuration panel on which ID corresponds to which font.	Integer	11
useCustomizingObject	Choose whether you want to use an object file to format print data instead of using the formatting provided by the application.	true, false	false
customizingObject	The name of a user-defined iSeries file that can be used to format the data for this device.	String	NONE
customizingLibrary	The name of the iSeries system library that contains the customizing object file.	String	*LIBL
printerModel	The printer model string of the printer that will be used for this session. See OS/400 documentation for printer models that are available on your OS/400.	String	*IBM42011

drawer1	Specifies the size of the paper in Source 1.	FF - None FE - Default used for printer 00 - No Change 01 - Letter 02 - Legal 03 - Executive 04 - A4 05 - A5 06 - B5 07 - Continuous 80 column form 08 - Continuous 132 column form 0E - A3 0F - B4 10 - Ledger	00
drawer2	Specifies the size of the paper in Source 2.	FF - None FE - Default used for printer 00 - No Change 01 - Letter 02 - Legal 03 - Executive 04 - A4 05 - A5 06 - B5 07 - Continuous 80 column form 08 - Continuous 132 column form 0E - A3 0F - B4 10 - Ledger	00
envelopeHopper	Specifies the size of the paper in the envelope feeder.	FF - None FE - Default used for printer 00 - No Change 06 - B5 09 - Monarch 0A - Number9 0B - Number10 0C - C5 0D - DL	00
asciiCodePage899	Choose true if your printer supports ASCII code-page 899. This is not resident on most printers.	true, false	false

Disabling functions

The following functions can be disabled using the DISABLE parameter:

Parameter Value	Function
CLRMAP	Color remapping
CUTPASTE	Cut/copy/paste
EMUL3270	3270 session
EMUL5250	5250 session
EMULCICS	CICS gateway session
EMULVT	VT session
FILEXFER3270	3270 file transfer
FILEXFER5250	5250 file transfer

EMUL3270PRT	3270 printer session
EMUL5250PRT	5250 printer session
KEYMAP	Keyboard remapping
MACRO	Macro record/play
SSL	Security
USERAPPLET	Startup-applets and run applet

Cached client installation parameters

Parameter name	Description	Default value	Valid values
CachedAppletNonNetworkLoad	When set to true the cached client recognizes that it is being loaded from a LAN drive or a CD, so it can present more helpful error messages and an end of installation message.	false	true, false
CachedClient	Must be set to true in cached client HTML pages. Host On-Demand uses this parameter internally to determine if it is in a cached environment. The Deployment Planning Wizard sets this parameter appropriately when building HTML pages.	false	true, false
CachedClientSupportedApplet	Applet that is started by HODCached.html.	com.ibm.eNetwork.HOD.HostOnDemand	valid class name
DebugCachedClient	Allows the cached client to output debug information.	false	true, false
DebugCodeModules	Determines if the cached client should load debug components instead of normal cached client components.	false	true, false
InstallerFrameHeight	Allows for customization of Installer.html file so you can add installation specific HTML to the installation page.	250	integer

InstallerFrameWidth	Allows for customization of Installer.html file so you can add installation specific HTML to the installation page.	600	integer
PreloadCodeModules	The list of components to be downloaded initially. If there is no parameter specified, the default will be the Host On-Demand default cached client.	HABASE, HAPRINT, HA3270, HA3270B, HA3270T, HA3270P, HA5250, HA5250B, HA5250T, HA5250P, HA5250E, HACICS, HAVT, HAVTT, HAVTB, HATHAI, HADBCS, HABIDI, HAMACRT, HAMACUI, HAXFER, HA3270X, HA5250X, HASSL, HACHTAU, HASLP, HAHOSTG, HALUM, HACOLOR, HAKEYPD, HAKEYMP, HACP, HODBASE, HODIMP, HODTH, HODBI, HODSSL, HODAPPL, HODMAC, HODIMG, HAHINDI, HA5250H, HAFNTIB, HAFNTAP, HAFNTAR, HAFNTHE, HAFNTTH, HODHLL	list of components
UpgradePercent	Sets the percentage of users who can upgrade when a new version of Host On-Demand is available.	100	0 (no one is upgraded) - 100 (everyone is upgraded immediately)
UpgradePromptResponse	Allows the administrator to answer the upgrade prompt now, later, or background without displaying the prompt to the browser. When this parameter is set to prompt, the browser displays the choice.	prompt	now, later, background, prompt
UpgradeURL	Specifies a URL that is used to determine whether a user should be upgraded when a new version of Host On-Demand is available. If the retrieved document contains the word upgrade , the user is upgraded	<none>	URL, or file name relative to code base



Preload Options

Use this panel to control the initial download size by specifying the Host On-Demand components to be included in the initial download. All other components will be downloaded as needed. If the user accesses a function for which the components have not been downloaded, the component will be downloaded at that time.



If you are using a Java 2 download client, you will **not** be able to download additional components after the first download. You should include any component you will need in the initial download. For more information on this, see [Limitations for Host On-Demand](#).

Select the checkbox beside a component to include it in the initial download. If you do not want a component included in the initial download, deselect it. Use the Select All and Deselect All buttons at the bottom of the panel to select whether all displayed components will be included in the initial download. Components that are indented cannot be selected until the component they are indented under is selected. For example, the 3270 File Transfer subcomponent cannot be selected unless its parent component (3270 Sessions) is selected.

If you are using the HTML-based model in the Deployment Wizard, an Auto Select button is available. If you click this button, it will automatically select the components needed to run the defined session types and features and remove the components not needed or disabled. For example, if a host session is defined, Color Remap will be included unless the Color Remap function is disabled in the Disable Functions panel. Other components, like Import/Export will be included unless both Import and Export are disabled in the Disable Functions panel. For other Deployment Wizard models, the default is that all components except the codepage components are selected and included in the initial download. If you do not want components included in the initial download, deselect them.

For example, if you are only using 3270 sessions, you should only download 3270 session components and those features that are used by 3270 sessions. Downloading any other session components would add unnecessarily to the size of the initial download. You may also wish to not include components for infrequently used functions in the initial download. Also, if you have disabled certain functions, you can deselect those components, as well, so they are not downloaded.

The size (in KB) of the components is displayed in parenthesis beside the component name. In addition, the panel displays a running total of the size requirement for all selected components. This running total is updated whenever a component is selected or deselected. There are three sizes associated with each component: the cab size for Internet Explorer, the jar size for Netscape, and the jar size for Java 2 browsers. You can select which value to display using the pulldown at the bottom of the panel. The default is to show the cab size unless the user has specified to create Java 2 pages in the Deployment Wizard. If so, the jar size for Java 2 will be displayed.

Components marked with an asterisk share files with other components. Therefore, removing a component marked with an asterisk may not reduce the download size if other components using the same files are still selected. The size indicated for these components is the maximum that the total download size will increase or decrease when selecting or deselecting them.

The following table lists all the components that share files with other components. This information is subject to change. If the information changes with a service update, the changes will be listed in the service update readme.

Component	Shares files with these components:
3270 Sessions	3270 Printer Sessions
3270 File Transfer	5250 File Transfer, All Macro Functions, Change Session Properties
3270 Printer Sessions	3270 Sessions, 5250 Printer Sessions, VT Sessions
5250 Sessions	5250 Printer Sessions
5250 File Transfer	3270 File Transfer, All Macro Functions, Change Session Properties
5250 Printer Sessions	5250 Sessions, 3270 Printer Sessions, VT Sessions
VT Sessions	3270 Printer Sessions, 5250 Printer Sessions
SSL Client Authentication Support	View Security
View Security	SSL Client Authentication Support

Change Session Properties	3270 File Transfer, 5250 File Transfer
All Macro Functions	3270 File Transfer, 5250 File Transfer
Chinese (Simplified)	Chinese (Traditional), Japanese, Korean
Chinese (Traditional)	Chinese (Simplified), Japanese, Korean
Japanese	Chinese (Simplified), Chinese (Traditional), Korean
Korean	Chinese (Simplified), Chinese (Traditional), Japanese
Arabic	Hebrew
Hebrew	Arabic



If your clients will be working in an environment in which they will be accessing multiple Host On-Demand configuration servers that may be at different levels, [special precautions](#) may be necessary to avoid problems.



Configuration Model

Specify how sessions are defined and managed on this page. You can choose from three different configuration models, which are defined below:

- [HTML-based model](#)
- [Configuration server-based model](#)
- [Combined model](#)

HTML-based model

Specifies that all session information is defined and managed in this HTML file. You have the same set of session options that you would have if using the configuration server.

Necessary configuration information and user preferences (for example, changes to color), if allowed, are stored locally on the user's machine. The configuration server is not used for sessions or preferences, and user IDs do not need to be created on the configuration server.

Choosing this model has several benefits:

- The configuration server is not used. Therefore, you do not need to start the Host On-Demand service manager unless you are using Host On-Demand services, such as the Redirector, OS/400 proxy, or license use counting (license use counting is enabled by default, but [can be disabled](#)).
- 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.
- You do not have to create or maintain Host On-Demand user IDs.
- There is no user logon.
- There are no firewall issues because you do not have to open a separate port to access the configuration server.

Choosing this model may have some limitations (depending on your environment):

- If users make changes to their personal configurations, those changes may not be available on other machines without physically copying them.
- If the administrator needs to define a large number of different configurations, it may become cumbersome maintaining all the HTML files.
- The Deployment Wizard does not run remotely. Therefore, there is no built-in mechanism for administering sessions remotely.

If this option is selected, the administrator uses the Deployment Wizard to define sessions in the HTML. Any changes the user makes are stored on the user's machine. (However, you can still choose to not allow users to save any session changes or to lock particular properties.) If the Administrator then updates the session data using the Deployment Wizard, those updates will be merged with any changes the user has made previously. In this case, all user preferences will be kept unless the administrator chooses to override those preferences.

HTML-based model is the default value.

Configuration server-based model

Specifies that all sessions are configured and managed on the configuration server using the Administration Utility and that each user has an ID on the configuration server where user-specific information is maintained.

Necessary configuration is stored in group or user IDs on the configuration server; user preferences, if allowed, are stored in the user's ID. One user ID per user is required on the configuration server.

Choosing this model has several benefits:

- It allows users to access their personalized configurations from any machine with network access because those

configurations are stored on the configuration server.

- For large numbers of different configurations, it might be advantageous to organize them using the configuration server group and user structures.
- It allows remote administration of sessions using the Administration Utility.

Choosing this model may have some limitations:

- There are very high administrative requirements to create and maintain all of the user IDs. (However, you can optionally have user IDs created automatically based on Windows usernames to help simplify this process).
- Performance may be diminished with large numbers of users accessing personalized configurations in the configuration server.
- Requires each user contacting the configuration server before using Host On-Demand.
- Users must log on. (However, users can be automatically logged on using their Windows username.)

In this model, the Administrator uses the Administration Utility to define session information for users and Groups.

If the Administrator then updates the session data using the Administration Utility, those updates will be merged with any changes the user has made previously. All user preferences will be kept.

Combined model

Like the configuration server-based model, specifies that all session information is defined and managed on the configuration server using the Administration Utility (users get their default sessions from a specified group on the configuration server).

However, unlike the configuration server-based model, necessary configuration information and user preferences, if allowed, are stored locally on the user's machine rather than on the configuration server in the user's ID. This option requires you to create at least one group on the configuration server.

Choosing this model has several benefits:

- No Host On-Demand user IDs to create or maintain.
- Performance may be better than using the configuration server because, while you still have to access the configuration server, you will not have large numbers of users accessing personalized configurations on the configuration server (some information is stored locally).
- Although the client attempts to contact the configuration server before each use, Host On-Demand will run using saved copies of the session configuration information if contact with the configuration server cannot be made.
- There is no user logon.
- For large numbers of different configurations, it might be advantageous to organize them using the configuration server group and user structures.
- It allows remote administration of sessions using the Administration Utility (however, you still have to use the Deployment Wizard for information in the HTML files).

Choosing this model may have some limitations (depending on your environment):

- If you make changes to your personal configurations, those changes are not available on other machines without physically copying them.
- Performance may be diminished with large numbers of users simultaneously accessing the configuration server to obtain their default configurations. However, users will not be accessing the configuration server to obtain or store their user preferences.

If this option is selected, the Administration Utility is used to create a group on the configuration server and create necessary sessions for that group. Then, the Administrator uses the Deployment Wizard to configure the HTML files that users will access, where the HTML files specify the configuration server group from which the default session configurations should be obtained. If the Administrator then updates the session data using the Administration Utility, those updates will be merged with any changes the user has made previously. In this case, all user preferences will be kept unless the administrator chooses to override those preferences.

Setting trace levels

Choose the amount of information you want to trace by selecting a trace level for each component:

1. Click Trace on the toolbar.
2. Select the function and component.
3. Select the trace level.

The tracing level applies to the selected component only. Select trace level 0 for no tracing. Trace level 1 captures the least amount of information and trace level 3 captures the most information.

Changing the trace settings (client)

1. Click Trace on the toolbar.
2. Click Settings.

Save to Java Console

Select On to display trace messages in the browser Java Console.

Save Location

Select where you want trace files saved. Selecting Server saves trace files in a default directory on the server and can only be viewed from the administrator window. Selecting Local allows you to choose where you want trace files saved.

Number of Trace Entries

Enter the number of trace and log messages to be logged to the trace buffer before wrapping starts.



Using Custom HTML Templates

By default, the Deployment Wizard generates HTML using a basic template installed with the Host On-Demand product. If you wish to modify the appearance of your Web pages, you can provide an alternate template to be used by the Deployment Wizard or modify the default template.

The default template that the Deployment Wizard uses is called Wizard.html, and it resides in the HOD publish directory. It contains fundamental tags for HTML formatting, a few markers for Host On-Demand use, and some appearance related information, such as banner and background specifications.

As long as the HTML formatting and the Host On-Demand markers in the template are not modified, the template can be customized in any way. For example, it can be updated to include a different banner, background, new images, new text, forms, or JavaScript. These new features will then be added to any HTML that the Deployment Wizard generates with that template.

You can either modify the default Wizard.html template and have the changes apply to each Deployment Wizard page created or edited, or you can create another template and selectively apply it to different Deployment Wizard pages.

Below is a set of specific steps to create and apply custom templates:

Creating a custom HTML template

1. To modify the default template, Wizard.html, first make a backup copy of the file (for example, Wizard.htmlbak). Otherwise, create a copy of Wizard.html, and edit the copy.
2. Modify the template in a UTF-8 compatible HTML editor to include customizations, such as different images and text. When editing the file, do not erase or modify the Host On-Demand marker statements:
<!--SUMMARY--><!--SCRIPTS--><!--APPLET--><!--STARTAPPLETPARMS--><!--ENDAPPLETPARMS--> Host On-Demand uses these statements to denote where to write various output information.

The tags STARTAPPLETPARMS and ENDAPPLETPARMS allow HTML parameters to be added to the template. All of the definitions between these two tags will be placed into the Host On-Demand applet section of the generated HTML.

A sample of the default Wizard.html template is shown below.

3. Save the file as a Web page with UTF-8 character encoding.

Sample default Wizard.html template:

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
<HEAD>
<META content="text/html; charset=UTF-8">
<!-- SUMMARY -->
</HEAD>

<BODY BACKGROUND="hodbkgnd.gif">
<CENTER>
<IMG src="hodlogo.gif" ALT="hodlogo.gif">
<P>
```

```
<!-- STARTAPPLETPARMS -->
<!-- ENDAPPLETPARMS -->

<!-- SCRIPTS -->
<!-- APPLET -->

</CENTER>
</BODY>
</HTML>
```

Note: Because the Host On-Demand cached client support uses a window onLoad event handler, you cannot use an onLoad event handler in the </BODY> tag. When both are present, it causes problems in the browsers. For download clients, the window onLoad event handler is not used; therefore, an onLoad event handler in the </BODY> tag can be used. Another window onLoad event handler can be used in all cases.

Applying the custom HTML template

If you modified the file Wizard.html, ensure that the customized template is located in the HOD publish directory and is named Wizard.html. This file will be applied to all Deployment Wizard pages created or edited (without having to specify a template).

If you want to apply a different custom template to a specific page that the Deployment Wizard generates, complete the following steps:

1. Open the Deployment Wizard and either select an existing Web page or choose to create a new Web page.
2. Go to the Additional Options panel of the Deployment Wizard and select Advanced Options.
3. On the Advanced Options panel, select the Other tab.
4. At the bottom of the Advanced Options panel, there is a field for entering the name and location of a custom HTML template.
5. Either type in the fully-qualified name of the new template or select Browse to find the template.
6. Once a template has been chosen, close the Advanced Options panel by selecting OK.
7. Save the Web page and close the Deployment Wizard. The template to be used for this Web page will be remembered by the Deployment Wizard for all subsequent updates.

Subsequent updates to your custom template

If you update the template after creating the HTML with the Deployment Wizard, it will be necessary to regenerate the HTML in order to pick up the changed template. This template is only used when the HTML is generated. To regenerate the file, open it in the Deployment Wizard, go to the last page, and select Create HTML.



Additional Options

Use this panel to specify any additional options that you want included in the HTML file.

Persist user changes?

When users make changes to session properties (for example, session size, placement, colors, toolbar customizations, and macros), these changes are associated with the browser window that was used to access the HTML and will remain in effect as long as that browser window remains active. If the user is allowed to persist changes (the default), modifications will be remembered the next time the user accesses the HTML. Otherwise, if No is selected, any session modifications will be lost when the user closes the browser window.

Cache Host On-Demand applet?

Specifies that the Host On-Demand components will be stored on the local disk the first time users download Host On-Demand. The next time they load this HTML page, all the components do not need to be downloaded from the server. Host On-Demand compares components on the local system to those on the server to see if any have been updated. Only updated components will be downloaded.

Selecting this option reduces subsequent download time because only updated components will need to be downloaded.



If your clients will be working in an environment in which they will be accessing multiple Host On-Demand configuration servers that may be at different levels, [special precautions](#) may be necessary to avoid problems.

Select Cache Options to see the [Cache Options](#) dialog, where you can specify options available for the cached client, such as controlling cached client upgrades.

Client Java type?

Specifies the format of HTML file to be used by browsers supporting different JVMs.

Java 1

If all of your users have Java 1-enabled browsers, specify this option to avoid the delay in detecting the Java level.

Java 2

Select Java 2 if all of your users have Java 2-enabled browsers.

Auto Detect

Select Auto Detect if your users have both Java 1 and Java 2-enabled browsers, or if you have Host On Demand deployed over the Internet so you are not sure what browsers your users have. Auto Detect allows all browsers to point to the same HTML file and receive either the Java 1 code or the Java 2 code, depending on their browser level.

If all three of the following apply:

- You have a previous version of Host On-Demand deployed using the cached client
- Your deployment uses the Configuration server-based model
- You want to control the cached client upgrade process using the cached client controls



you must select Java 1 until your users get upgraded to Host On-Demand 7. The Auto Detect HTML file format is not compatible with client code from previous versions of Host On Demand. If any one of the above does not apply, you can select Auto Detect.

Select Advanced Options to see the [Advanced Options](#) dialog, where you can configure display options, number of sessions allowed, problem determination, language, and additional HTML parameters for this HTML file.

Select Preload Options to see the [Preload Options](#) dialog, where you can configure the size of the initial download by selecting which components are included in the initial download. All other components will be downloaded as needed.

If you have selected the [Configuration server-based model](#) or the [Combined model](#) for your session configuration, select Server Connection Options to see the [Server Connection Options](#) dialog, where you can specify a different Configuration

Server port, or configure the configuration servlet. If you are running [Host On-Demand through a firewall](#), using the configuration servlet eliminates the need to open an extra port for the configuration server.



Cache Options

Use this panel to specify the options available for the cached client.

The Cache Option dialog allows you to specify the following options:

Debug cached client installation process?

Debugs the process of downloading and installing the cached client. You should only use this option if working with IBM Service.

Enter the size of the progress indicator frame

Specifies the width and height (both in pixels) of the progress indicator frame for the download process. If you are going to customize this frame, you may wish to resize it.

The default width is 550 pixels.

The default height is 250 pixels.

When an upgraded version of the cached client is available

Specifies how to control user upgrades when a new version of the cached client is available. If you have a large number of users that will be accessing this page at the same time, having them all upgrade at once may put a strain on your network.

For load-balancing purposes, you can control the upgrade process by specifying that only a certain percent of users can upgrade at a time. If you specify that only a certain percent of users can upgrade at a time, when the user accesses the page, a random number is generated. If this random number falls between 0 and the specified percent, they are allowed to upgrade. If it does not, then the upgrade process is postponed until the next time the user accesses the page, at which time another random number is generated. As the number of users who have not been upgraded using this process declines, you may wish to raise the percentage to 100 to ensure that all users are upgraded.

You can also specify two independent percentages. One of the percentages is effective only during a specified time period. The other percentage is the default for any time outside of the specified time period. You may want a lower percentage during daytime hours because of increased network traffic and a higher percentage for hours when network traffic decreases. The clock used to compute the current time is always the client workstation and not the server, so you should account for different time zones. If you enable this specified time period, the client determines if the current time is between the specified start and end times. If it is, the client uses the percentage that you specified for that time period. If the current time is not between the specified start and end times, it uses the default percentage. You do not have to specify a start and end time.

You can also control the upgrade process by creating a script (such as a PERL script) that will determine whether the user should be upgraded. For example, the user's IP address could be queried, and if it falls within a certain range, the user can be upgraded. The script must return the string "upgrade" for the user to be upgraded. Enter the URL to the script file to use this option.

The default is to allow all users to upgrade. To disable the clients from upgrading, set the upgrade percentages to 0.

Upgrade option

Specifies how to upgrade the cached client.

If you choose Upgrade in foreground, the user will be forced to upgrade and cannot use the cached client until the new version is installed. They will have to restart the browser after the new version is installed.

If you choose Upgrade in background, the user will be forced to upgrade, but can still use the older version of the cached client while the new version is being downloaded. This may be preferred when the user is working over a slow connection and can't wait until the upgrade process is complete to begin their work. They will have to restart the browser once after the new components are downloaded and again after the new components are installed.

If you choose Prompt user, the user will be prompted whether to upgrade in the foreground or background. They can also choose to cancel and not upgrade at that time. If they cancel, they will be prompted again to upgrade the next time they

load this page until they do upgrade.

The default is to prompt the user.



Advanced Options



Use this panel to define display, message, and additional parameters for this HTML file.

Display

Use the Display page to configure how the Host On-Demand client window appears. You can also configure how many concurrent sessions each user can have open. When this number is reached, a user will not be able to open any more sessions (regardless of session type) until some currently-opened sessions are closed.



The Autosize to browser function is not supported on Netscape 6.1 browsers.

Other

Use the Other page to specify whether or not to include problem determination components, such as the Trace Facility, View Log Messages, and System Properties. (You will probably only need these components when working with IBM service to troubleshoot a problem.)

To use [IPMon](#), or to use [trace in automatic mode](#), you will need to configure additional parameters.

You can specify the language to use for all client desktop and session frame messages. If users with different languages will be accessing this HTML file, you should select Use the System Locale from the Select Language list.

If you are publishing files generated from the Deployment Wizard to a location other than your Host On-Demand publish directory, specify the URL of your Host On-Demand publish directory in the Codebase field. This name must either be 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/). For more information on how and why you would want to publish files generated from the Deployment Wizard to a location other than the publish directory, see [Setting up a separate user publish directory](#).

You can also include banners, backgrounds, images, and other HTML in your Host On-Demand Web page by specifying a custom HTML template on this page. Click Browse to choose the HTML template that you want to use. The template is applied to the Web page when it is created at the end of the Deployment Wizard. For information on creating custom HTML templates, see [Using Custom HTML Templates](#).

Select Enable Session Manager JavaScript API if you want to use JavaScript APIs to manage host sessions and text-based interactions with host sessions. These public APIs allow you to communicate with host sessions that are embedded in a Web page.

If you select Enable Session Manager JavaScript API, the Deployment Wizard adds HODJSAPI.js to your HTML file.

There are four sets of APIs:

- Session Manager APIs
- Presentation Space APIs
- Host On-Demand Functions APIs
- Error Reporting APIs

For details about how to use these JavaScript APIs, refer to the [Session Manager API Reference](#).

Additional Parameters

The Deployment Wizard automatically includes HTML parameters for all options shown in the wizard. However, if you want to include options that are not shown in the wizard, you can use the Additional Parameters page to add the necessary parameters to include those options.

You should not manually add these parameters to the HTML file (for example, using a text editor), or they may be lost the next time you open the file with the wizard. When adding parameters to this page, you should not include quotes around the names and values.

These are some of the additional HTML parameter names and values that you may find useful:

- [CustomKeyFunctionX](#)
 - [Disable](#)
 - [DisableSupport](#)
 - [DoNotPrefillUser](#)
 - [HideHODDesktop](#)
 - [IgnoreWellKnownTrustedCAs](#)
 - [Save](#)
 - [ShareCachedClient](#)
 - [SkipConfigProperties](#)
 - [SupportHTML](#)
 - [3270InputAreaIndication](#)
-

Name: CustomKeyFunctionX

Value: *function identifier|function data*

Description: Customize the list of functions that a key or key combination can be mapped to using Keyboard Remap.

Keyboard Remap allows you to remap key functions by selecting the key you want to remap, then selecting the new function you want that key to perform. The list of available key functions is limited, by default, to a set of predefined key functions; however, you can customize this list with additional functions. When this file is loaded, you can go to the Keyboard Remap dialog, choose Custom Functions from the Category list, and your custom functions will appear in the list for you to map to a key.

Here is an example of parameters that add key functions to display, respectively, a character that you cannot normally display, automate a login with user ID and password, and automate a logout.

Name: CustomKeyFunction1 **Value:** Ctrl-A|^A

Name: CustomKeyFunction2 **Value:** Login|myuserid[tab]mypw[enter]

Name: CustomKeyFunction3 **Value:** Logout|logout[enter]

The value for the NAME field is always CustomKeyFunctionX, where X is the ordinal of the defined function. Host On-Demand iterates through the custom key function list, starting with 1 and continuing until no CustomKeyFunction value is found.

You must begin with CustomKeyFunction1 and continue in increments of 1. If the list is broken, for example, skips from CustomKeyFunction2 to CustomKeyFunction4, all values after CustomKeyFunction2 are discarded.

The VALUE consists of both the function identifier to the left side of the | and the function data to the right. The identifier displays in the Keyboard Remap function list box. The data is what the emulator processes when the remapped key is pressed.

There are three rules to keep in mind when encoding the value field.

- **Bracket encoding**

Host On-Demand supports the ability to process SendKeys mnemonics, so to send a bracket, you must use all double brackets `[[]]`. Single open and close brackets `[]` are translated as field boundaries for SendKeys mnemonics. For more information about SendKeys, refer to Appendix A and the ECLPS class in the Host Access Class Library documentation.

- **Carat encoding**

The carat (^) is used to send characters that cannot be displayed. Place a ^ in front of any character with a value greater than or equal to A (hex 41, decimal 65) to translate to that value minus hex 40 or decimal 64; for example, `"^A"` = hex 01, `"^B"` = hex 02, and so on. The only way to get a ^ into the datastream is to double it. In other words, `^^` is equal to ^ in the datastream.

- **Unicode encoding**

You can use Unicode encoding to put displayable and non-displayable characters into the datastream. Unicode encoding uses the format `\uxxxx` where `xxxx` is two hex bytes. The value for the escape character is `\u001b`.

Related topics:

- [IBM Screen Customizer parameters](#)
-

Name: Disable

Value: lum

Description: This disables [license use counting and License Use Management server](#) reporting for the particular HTML. By default, Host On-Demand clients will report to the configuration server when a session is launched and periodically thereafter for the duration that the session is open. The client requires direct port access to the configuration server for its reporting. If this parameter is included, the client will no longer report to the configuration server for license use counting purposes.

Name: DisableSupport

Value: true

Description: Causes the Support option of the Help menu item for the Session window to be disabled. This is useful in cases where customers do not wish to have their users contacting IBM support directly. A related parameter, [SupportHTML](#), can be used to specify an alternate set of text to display when the user selects the Help/Support option.

Name: DoNotPrefillUser

Value: true

Description: **For Configuration server-based model only.** Causes the logon panel to come up with a blank user ID field. If this parameter is absent, the default is to fill in the user ID with the username requested from the system.

Name: HideHODDesktop

Value: true

Description: Hides the Host On-Demand desktop and session tabs once an embedded session starts. Do not set this parameter if you have multiple sessions running and you are not using the Session Manager JavaScript API. To prevent users from interacting with the Host On-Demand desktop, configure your session to Auto-Start.

Name: IgnoreWellKnownTrustedCAs

Value: true

Description: Prevents Host On-Demand from loading the WellKnownTrustedCAs.class file.

Name: Save

Value: *directory location*

Description: **For HTML-based and Combined models only.** Specifies the base directory location where local user preferences will be stored. The directory must exist or the user will get an error.

Examples of valid Save directories are as follows:

- Absolute paths (for example, `C:\hod\prefs` on a Windows operating system or `/hod/prefs` on a Unix-based operating system) are allowed. Mapped network drive letters can also be used in the absolute path.
- Remote computer names or IP addresses are allowed as long as the following condition is met: the user's computer must already be remotely connected and authenticated to the computer in the Save parameter (for example, when network drives are mapped; however, a mapped drive is not a prerequisite for the Save parameter to work).

Following are two examples of Save values to remote computers:

- `\\DevGroup1\prefs`, where *prefs* is a shared folder on a computer named DevGroup1.

- \\123.45.67.89\prefs, where *prefs* is a shared folder on a computer with an IP address of 123.45.67.89.
- Relative paths (for example, \users\preferences on a Windows operating system or ../preferences on a Unix-based operating system) are also valid. On Windows operating systems, the relative path is appended to the home directory to make an absolute path. On Unix-based operating systems, the relative path is relative to the user's current working directory.

The Save directory is only a base location for storing user preferences. Preferences will be stored in the following subdirectories within the Save directory (these folders are created dynamically): *user login/profile ID/HODData/web page name*.

Name: ShareCachedClient

Value: true

Description: Enables users on Windows 2000 and Windows XP multi-user machines using Internet Explorer with Microsoft JVM to share a single image of the cached client. Only the first user will download the cached client code. Subsequent users may use or update this code without requiring a full download.

If you have users who are Restricted Users, see [Internet Explorer cached client support for Windows 2000 and Windows XP](#) for more information on using this parameter.

Name: SkipConfigProperties

Value: true

Description: Prevents the reading of HTML parameters from the *config.properties* file.

Any parameters in the *config.properties* file (in the Host On-Demand publish directory) will apply to all HTML files, unless the HTML file specifically overrides the parameter value. If for some reason you want to prevent the HTML file from reading values in *config.properties*, you can use this option.



Setting global values: If you want to set global values that apply to all HTML files, you can specify any of these additional parameters in the *config.properties* file in the Host On-Demand publish directory. All Host On-Demand applets read the *config.properties* file. This provides an easier way of setting global HTML parameters than specifying them in each HTML file. Any of these HTML parameter can be set this way, and as long as the value is not specified in the HTML file, the value from the *config.properties* will be used.

Name: SupportHTML

Value: URL of HTML file to display when user selects Support option of Help menu item

Description: Causes the specified HTML file to be displayed when the Support option of the Help menu item for the Session window is selected.

If this parameter is not specified, the help page, which provides IBM contact information, is displayed. A related parameter, [DisableSupport](#), can be used to disable the Help/Support option.

Name: 3270InputAreaIndication

Values:

- Underdot,DisplayAndNonDisplay
- UnderDot,NonDisplay
- UnderDot,Display
- UnderLine,Display
- UnderLine,DisplayAndNonDisplay
- UnderLine,NonDisplay
- 3DLowered,DisplayAndNonDisplay
- 3DLowered,Display
- 3DLowered,NonDisplay

- 3DRaised,DisplayAndNonDisplay
- 3DRaised,Display
- 3DRaised,NonDisplay

Description: 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.



Host Sessions

Use this panel to define the host sessions that you want included in the HTML file. You can choose from the following types:

- 3270 Display
- 5250 Display
- VT Display
- CICS Gateway
- 3270 Printer
- 5250 Printer
- FTP

To add a session, select a host type, enter a session name and destination address (optional), and click Add. To configure other properties of the sessions, select a session and click Properties.

On this panel, you can also choose the order that your sessions will initially be displayed on your Host On-Demand client. To do this, highlight the session that you want to move, and then select the up or down arrow button to the left of the host session list box. Note that once a user accesses the HTML file, reordering the Deployment Wizard sessions on the server will have no effect because all the configuration information, including the order of the session icons, is stored locally on the user's machine.

To configure run-time options, such as window size and placement, colors, toolbar customizations, macros, etc., select a session and click Start. Any changes you make to the session will be saved as part of the HTML file.

Select Disable Functions to see the [Disable Functions](#) dialog, where you can define which functions are enabled and which are disabled to end users. These settings apply to all sessions defined in this HTML file.

- [Disabling Functions: Client Window](#)
- [Disabling Functions: Connection](#)
- [Disabling Functions: Appearance](#)
- [Disabling Functions: Macro](#)
- [Disabling Functions: File Transfer](#)
- [Disabling Functions: FTP](#)
- [Disabling Functions: Printer](#)
- [Disabling Functions: Preferences](#)
- [Disabling Functions: Other](#)



Disable Functions

This page allows you to define which functions are enabled and which are disabled to end users. This applies to all sessions defined in this HTML file. The default is that all functions are enabled.

When you choose to disable functions, you prevent users from accessing those functions by removing them as options from the session menus. Note that if you choose to enable functions, they will only be enabled in session types that have that function. For example, if you enable functions on the Printer tab, this only enables these functions for printer sessions.



If you disable a function, you might want to deselect the corresponding component in the Preload Options panel so components for this disabled function are not included in the download.

The following options are available from this dialog:

- [Disabling Functions: Desktop](#)
- [Disabling Functions: Connection](#)
- [Disabling Functions: Appearance](#)
- [Disabling Functions: Macro](#)
- [Disabling Functions: File Transfer](#)
- [Disabling Functions: Printer](#)
- [Disabling Functions: Others](#)

Using DWunzip



Web pages from the Deployment Wizard can be distributed to servers in a more automated process using the DWunzip tool. This tool is installed on all platforms supported by Host On-Demand, including OS/390, Unix-based systems, and iSeries. DWunzip will unzip the Deployment Wizard .zip file, place the Deployment Wizard files in the appropriate directories, append any necessary file extensions for OS/390, and set file permissions and ownership on the files and directories for non-Windows platforms.

You can use the DWunzip tool to deploy files onto any server running Host On-Demand. The administrator must first transfer the .zip file created by the Deployment Wizard to the Host On-Demand publish directory on the target server. Once on the target server, run DWunzip, which will automatically complete the remaining steps necessary to deploy the files on that server.

DWunzip is located in the following directories:

- On non-Windows platforms: /Host On-Demand install directory/lib/samples/DWunzipCommandFiles
- On Windows platforms: /Host On-Demand install directory/lib/samples/DWunzip/

DWunzip is a command-line program that requires one parameter: the name of the .zip file to be extracted. The .zip filename does not need a path or .zip extension associated with it; otherwise, an error message and usage statement will result. Other information, such as the location of the JRE or of the Host On-Demand publish directory on the server, is contained in the command file and must be changed by the administrator (if they are different than the default values supplied in the file).

To run DWunzip, do the following:

1. For all platforms, to run DWunzip, you must be able to write to the Host On-Demand publish directory.
2. Ensure that the .zip file created by the Deployment Wizard is located in the publish directory on the target server. If it is not, copy it to the publish directory on the target server.
3. Open the command file, DWunzip.cmd, and verify that the target paths specified within it are correct.
4. Open a command prompt on the target server.
5. Change the current working directory to the directory location of the DWunzip tool.
6. On non-Windows platforms, make sure the DWunzip command has execute permissions.
7. Run the appropriate DWunzip command file for your operating system. For example, AIX users should run DWunzip-AIX *zipfile*, where *zipfile.zip* is file you want to deploy.

When DWunzip is running, it will display status messages to the command line showing the files and folders that were extracted, overwritten, or created. It will also display a message when the command is complete. If you have run this tool once and are running it again on the same .zip file, you will be asked whether you would like to overwrite the files. If you do, the files will be overwritten. If you do not, the tool will close and nothing will be overwritten.

The client window

When you log on, the client window opens. It has two areas:

- [Configured sessions](#)
This contains an icon for each of the sessions that the administrator configured for you, or that you added.
- [Active sessions](#)
This area contains sessions that you started. After you start a session, a lightning bolt and the name and ID of the session appears. If a session is started but not connected, the bolt has a break in it.

The Configured Sessions area

The Configured Sessions area appears after you log on and remains in your browser while you are running Host On-Demand. If you close your browser, you will also close all Host On-Demand sessions.

[Starting a session](#)

[Modifying a session](#)

[Copying a session](#)

[Deleting a session](#)

[Bookmarking a session](#)

[Arranging session icons](#)

Starting a session

Double-click the icon of the session you want to start.

Modifying a session

1. Right-click the session's icon to display the pop-up menu.
2. Click Properties.
3. The configuration window appears. Modify the fields as necessary, then click OK.

Copying a session

1. Right-click the session's icon and click Copy.
A new icon appears in the Configured Sessions area with a number added to the beginning to indicate it is a copied session. For example, if the original session name is **3270 Session**, the name of the first copied session is **1:3270 Session**. The new session has the same configuration as the original session you copied.
2. Right-click the new icon and click Properties to make any changes, such as the session name.
3. To make another copy, right-click the session's icon, either the original or the copied session icon, and click Copy again.

Deleting a session

1. Right-click the session's icon and click Delete.
A confirmation window asks if you really want to delete the session.
2. Click Yes.

Bookmarking a session

You can create a bookmark in your browser for a session. This lets you start a session that has already been configured.

1. Right-click the session's icon.
2. Click Set Up Bookmark, then choose Run in a separate window or Run in a browser window. For more information about these choices, click Help.
3. Click OK. You are then reminded to create the bookmark.

Next time you want to start that session, just click the bookmark.

Arranging session icons

To arrange your configured sessions by name or type, right-click in the Configured Sessions area and select Arrange Icons > by Name or Arrange Icons > by Type. This option is only available for models using local preferences, namely the HTML-based model or the Combined model. If you have created sessions using the Configuration server-based model, this option is not available.

The Active Sessions area

[Starting another identical session](#)

[Connecting or disconnecting a session](#)

[Closing a session](#)

[Switching to another session](#)

Starting another identical session

1. Right-click the session name.
2. Click **Run the Same**.

Connecting or disconnecting a session

1. Right-click the session name.
2. Click Connect or Disconnect.

Closing a session

1. Right-click the session name.
2. Click Close.

Switching to another session

Double-click the name of the session to which you want to switch. If the session to which you want to switch is minimized, it is not restored.

Related topics

- [Adding sessions](#)



Using Session 1 and Session 2



sample HTML files

Session 1 and Session 2 are HTML files that Host On-Demand Version 5.0 and earlier provided as examples for creating customized HTML files for users. Now, you can use the [Deployment Wizard](#) to accomplish complete HTML functionality, and we no longer recommend that you use these sample HTML files. However, we continue to provide them as samples for those users who are familiar with them.

These sample files are called session1.html and session2.html, and are located in the **doc/samples/html** directory. These files do not support new functions added to Host On-Demand since version 5.0.



Session 1 and Session 2 were the HTML precursors of the Deployment Wizard's Combined and HTML model pages, respectively.

You cannot open more than one customized file in the same browser window at one time, though you can use **Run the Same** to start more than one identical session. If you want to open more than one customized file, you must use a separate browser window for each.

Related topics

- [Using Session 1 to bypass logon and start a configured session](#)
- [Using Session 2 to configure and start a session](#)
- [Using Session 1 and Session 2 to disable functions](#)
- [Using Session 1 and Session 2 to create buttons for sessions](#)

Security tab



[Enable Security](#)

[Security protocol](#)

[Telnet-negotiated](#)

[Server Authentication](#)

[Add MSIE Browser's Keyring](#)

[Send a Certificate](#)

[Certificate Source](#)

[URL or Path and Filename](#)

[Select File](#)

[Certificate Name](#)

[Add Name](#)

[How Often to Prompt](#)

[Retrieve Certificate before Connecting](#)

[Lock](#)

Enable Security

Enables security between the workstation and either a telnet server that supports security or the Redirector.

Note: If Enable Security and [Enable SLP](#) are both set to Yes, a connection can be established only to servers that are enabled for security.

The remaining options are greyed out unless Enable Security is set to Yes.

Security Protocol

Select one of the following security protocols from the drop-down menu:

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.

SSL

Enables SSL version 3.0 security. Select this protocol only if the server cannot correctly negotiate a TLS connection.

Telnet-negotiated

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.

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 via 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

The certificate can be kept 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

This button invokes a dialog to allow browsing the local file system for the file containing the certificate.

Certificate Name

This drop-down box allows selection of a certificate from those available; optionally you may choose to accept any certificate trusted by the server.

Add 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 box 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 button is turned on, the client will access its certificate before connecting the server, whether the server requests a certificate or not. If this button 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.

Lock

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Related topics

- [How TLS and SSL security work](#)
- [Configuring TLS and SSL](#)
- [Telnet-negotiated security overview](#)
- [Telnet-negotiated security](#)
- [Configuring Telnet-negotiated security](#)
- [Client Authentication](#)



Server authentication



When you define a secure connection, Host On-Demand offers three options on the Security tab: Enable Security, Security Protocol, and Send a Certificate ([client authentication](#)).

Enable Security

Click Enable Security to enable server and client authentication.

Security Protocol

Security Protocol specifies the method used for client and server authentication. Select one of the following options:

TLS

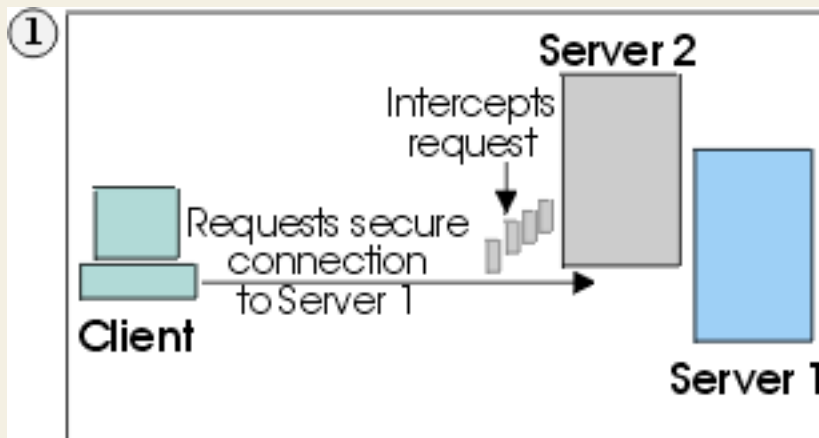
Transparent Layer Security (TLS) protocol. The TLS option creates a standard TLS connection between the client and the server. The client contacts the server by sending a communication known as a handshake, which enables the client and server to authenticate to each other and specify the type of encryption that is used during the session. All data exchanged between the client and server during the session is encrypted and cannot be read by a third party. In addition, the protocol includes a message integrity check to ensure the integrity and reliability of transmitted data.

SSL

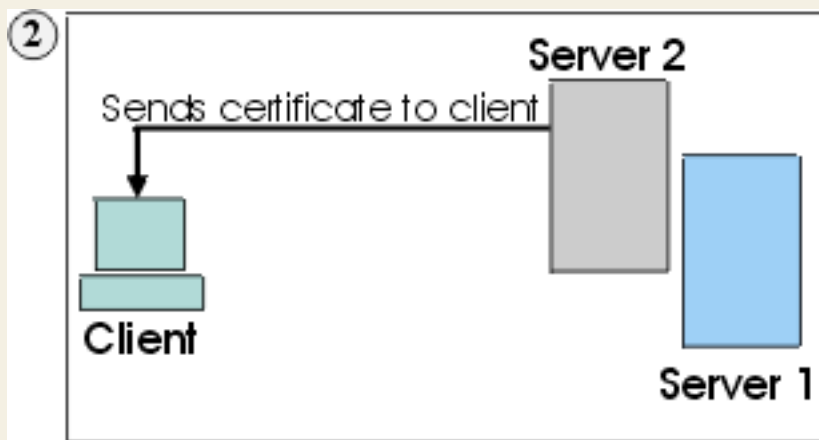
Secure Sockets Layer (SSL) protocol. The SSL option creates a standard SSL connection between the client and the server. The client contacts the server and checks to make sure that the server has a valid certificate. This type of connection ensures that all data exchanged between client and server is encrypted, and is therefore not readable by a third party on the Internet.

Server Authentication (SSL)

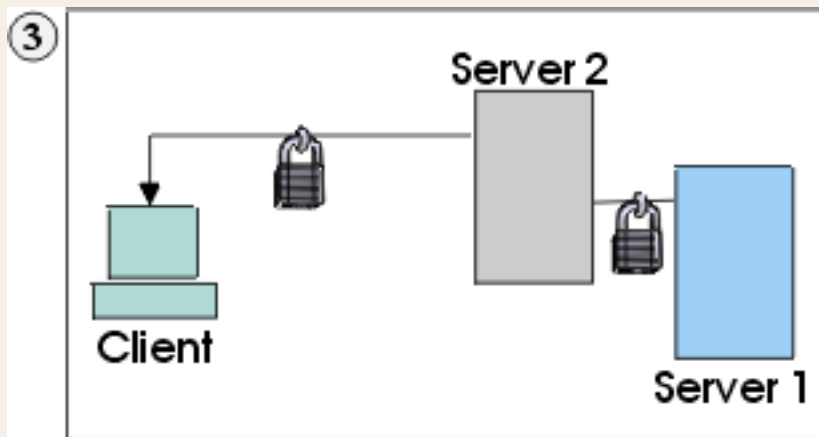
SSL by itself does not guarantee that the client is communicating with the correct server. To illustrate the risks involved with this protocol, consider the following scenario. There are two servers, **Server1** (hod.S1.com) and **Server2** (hod.S2.com), and one client, **Client**. Both servers have valid certificates from a CA that the client trusts. Client wants a secure session with Server1, but Server2 wants to eavesdrop on their communication, and is physically located in such a place that it can do so. The scenario goes as follows:



Client sends a request for an SSL session to Server1. The request (and all subsequent traffic) actually goes through Server2. Instead of forwarding Client's request to Server1, Server2 responds directly to the request by sending its own certificate to Client.



Client receives Server2's certificate and checks its list of trusted CAs. Since Server2's certificate is signed by the same CA as Server1's certificate, Client accepts the certificate and creates a secure session with Server2.



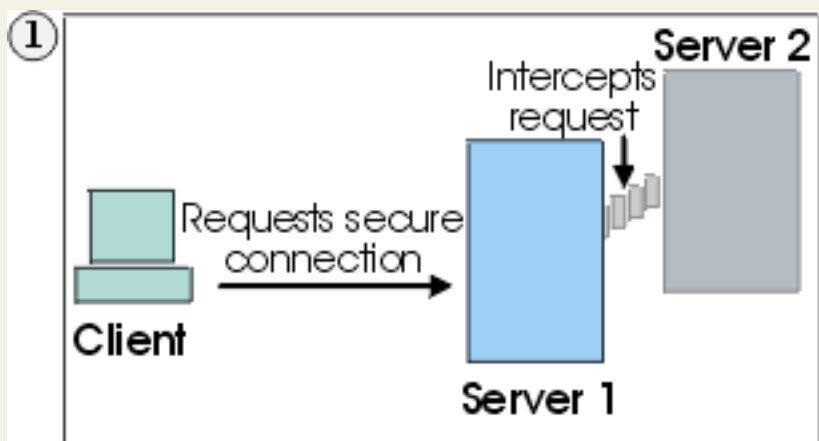
Having completed the secure session with Client, Server2 requests and creates its own SSL session with Server1. From this point, Client sends encrypted information to Server2. Server2 decrypts the information, re-encrypts it, then sends it to Server1. It does the same for information flowing in the opposite direction. The result is that, although all data is encrypted when it flows over the Internet, Server2 is able to read it, and even change it.

To help avoid this danger, the Server Authentication (SSL) option is provided. When this is switched on, the client, after making sure that the server's certificate can be trusted, checks whether the Internet name in the certificate matches the Internet name of the server. If they match, the SSL negotiation will continue. If not, the connection ends immediately.

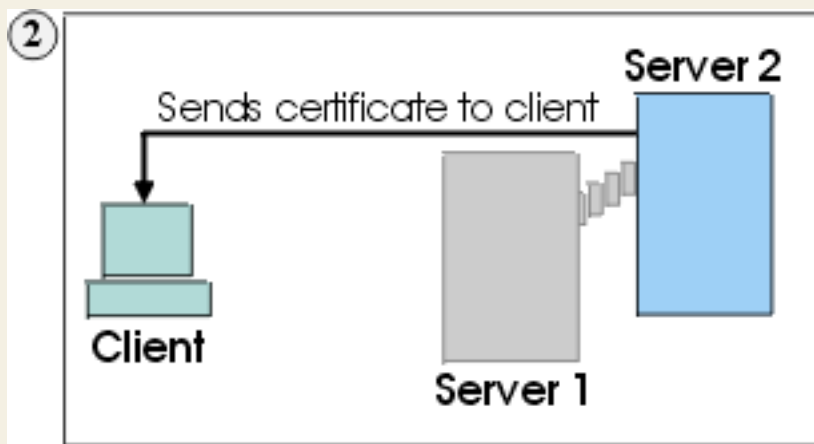
For this check to be valid and give a positive result, two conditions must be met:

1. The client must be locally-installed. A client downloaded using http [cannot be trusted for server authentication](#). If server authentication is of vital importance, you should use only locally-installed clients or use https on your Web server.
2. The common name in the server's certificate must match its Internet name.

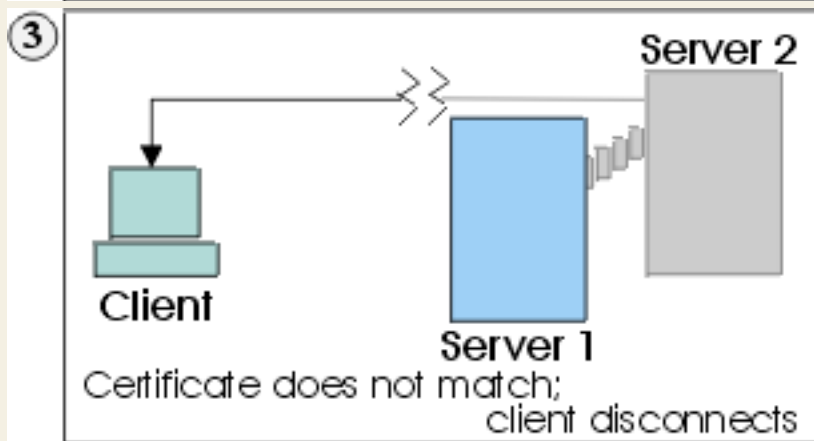
With Server Authentication (SSL) enabled, the security scenario would proceed as follows:



1. Client sends a request for an SSL session to Server1. The request (and all subsequent traffic) actually goes through Server2. Instead of forwarding Client's request to Server1, Server2 responds directly to Client's request by sending its own certificate to Client.



2. Client receives Server2's certificate and checks its list of trusted CAs. Since Server2's certificate is signed by the same CA as Server1's certificate, Client accepts the certificate and creates a secure session with Server2.



3. After the secure session has been completed, but before any real data has been sent or received, Client compares the Internet name in the certificate it received (hod.S2.com) with the name of the server it wants to talk to (hod.S1.com). Since they do not match, Client knows that the connection should not continue and disconnects it.

Related topics

- [Obtaining a server certificate](#)
- [Making server certificates available to clients](#)
- [How TLS and SSL work](#)

Security limitations



Although breaches of security on the Internet are infrequent, it is important to be aware of the inherent limitations of any Internet security system. The following information is not unique to Host On-Demand; it applies to most Internet applications that use http. None of this information applies if your Web server uses secure http (https).

For Host On-Demand, SSL security is still provided even when Server Authentication is disabled.

A common SSL connection between a client and a server works as follows:

Using a CA-signed certificate:

1. The client contacts the server.
2. The server sends its CA-signed certificate to the client.
3. The client checks its list of trusted CAs to see if the CA that signed the server's certificate is in the list and therefore can be trusted. If so, the SSL negotiation continues; if not, it fails immediately.

Using a self-signed certificate:

1. The client contacts the server.
2. The server sends its self-signed certificate to the client.
3. The client checks its list of self-signed certificates to see if the server's certificate is in the list and can therefore be trusted. If so, the SSL negotiation continues; if not, it fails immediately.

Why You Must Be Careful

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, on which Host On-Demand is loaded directly from the client's hard disk, that list is kept on its local hard disk. This is considered adequately secure.

However, for a download client, on which the client is really just a browser that downloads all its code from the server using http, 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, security is breached. One way to avoid this problem is to use https rather than http, because https ensures that the browser really is connected to the correct server.

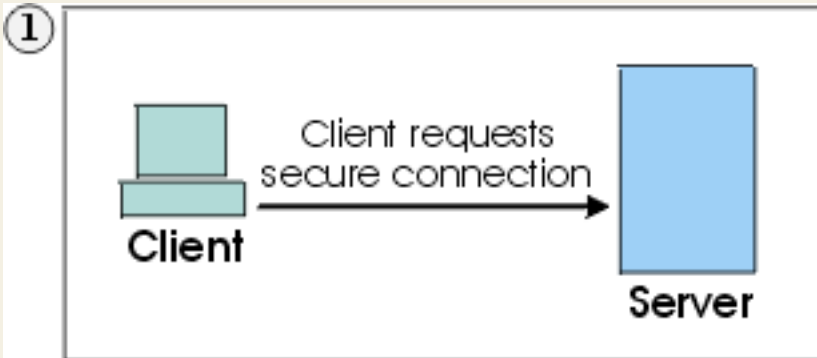
Related topic:

- [How SSL works](#)
- [Server authentication](#)

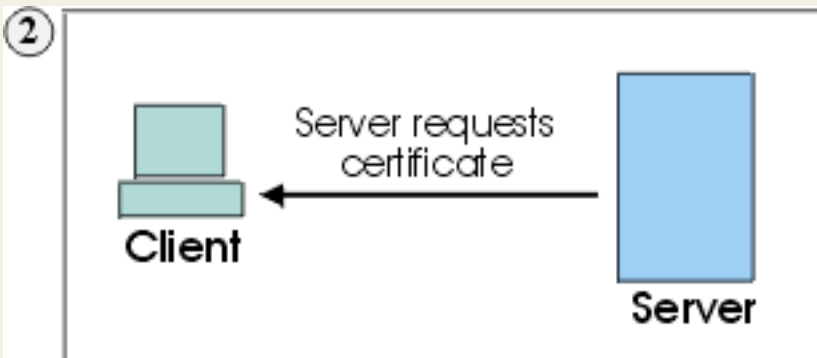
Client authentication

Client authentication is similar to [server authentication](#) except that 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. The later versions of the IBM Communications Servers (CS/NT, CS/AIX, etc.) all support client authentication.

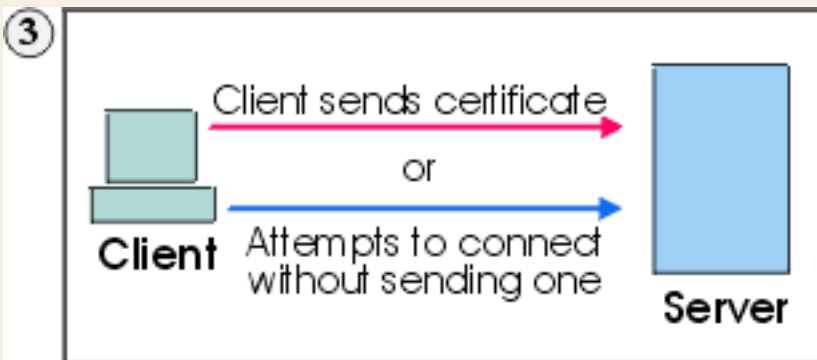
When a server requests a certificate, the client has the option to send a certificate or attempt to connect without it. The server allows the connection if the client's certificate can be trusted. When a client attempts to connect without a certificate, the server might give the client access but at a lower security level.



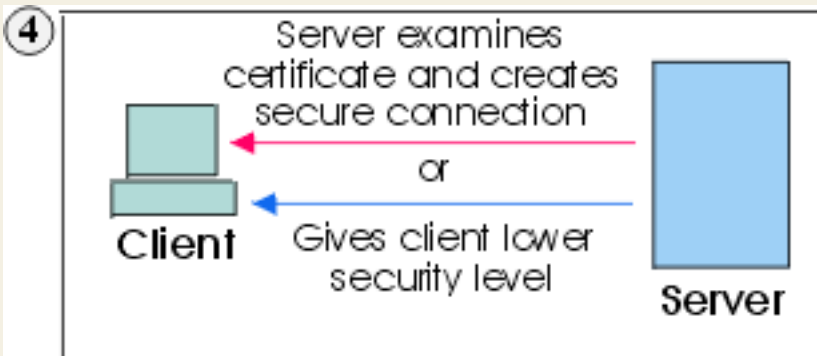
Client sends a request for an SSL session to Server.



Client receives Server's certificate and checks its list of trusted CAs. Since Server's certificate is signed by a trusted CA, Client accepts the certificate. Server asks Client for a certificate that will identify the Client.



Client sends a certificate or tries to establish a session without one.



If Client sends a certificate, Server checks its list of trusted certificates. If the Client can be trusted, the secure session is established. If Client does not send a certificate, Server establishes a secure connection at a lower level of security.

To configure client authentication:

1. [Obtain certificates for clients.](#)
2. Securely send the certificate files and their passwords to the clients, or install the certificates in the clients' browsers or security devices.
3. [Configure clients to use client authentication.](#)

When a certificate expires, follow the renewal procedures specified by the CA for that certificate.

Related topics

- [How SSL works](#)
- [Server authentication](#)

Default Characters and Functions



Alternate Cursor - Changes the shape of the cursor from underscore to block or from block to underscore.

Alternate View - Switches between basic and alternate character viewing modes in a DBCS session. For example, you can switch a viewing mode from the EISU KANA character set to the EIKOMOJI character set or vice versa. This switch affects the character view but not affect the character input.

Attention - Interrupts the application program; available only when the connection-method is SNA. If the connection method is not SNA, X-f (Minus Function) appears in the operator information area.

Backspace - Moves the cursor one position at a time to the left and deletes the character at the cursor position. All characters to the right of the cursor (in the same unprotected field) shift one position to the left.

If you press this key when the cursor is in a protected field, X <-o-> (Go Elsewhere) appears in the operator information area.

Backtab - Moves the cursor back to the first position in the unprotected field. When the cursor is not in an unprotected field or is in the first position of an unprotected field, it moves to the first position of the previous unprotected field.

If the screen is unformatted or does not contain unprotected fields, the cursor moves to the top left corner of the screen.

Backtab Word - Moves the cursor to the first character of the current word. When the cursor is already on the first position of a word, the cursor is moved to the first position of the previous word.

Beginning of Field - Moves the cursor to the first position of the field containing the cursor.

Clear Fields - Deletes text in the presentation space and replaces all unprotected fields with blanks. Protected fields are not changed. Nulls in the presentation space are left as nulls.

Copy Functions



- The Copy, Copy Append, and Copy as Table functions are only available if you are using a browser or Java Development Kit (JDK) version 1.1 or higher and if you have system clipboard access.
- If no area is marked, the Copy functions duplicate the entire session window.
- The Copy functions do not duplicate host attributes such as color and intensity.

Copy - Duplicates the marked area into the system clipboard without removing (clearing) it from the display.

Copy Append - Duplicates the marked area and appends it to the contents of the system clipboard.

Copy as Table - Duplicates a marked area that is formatted into columns and places it as a table into the system clipboard.

Cursor Down - Moves the cursor down one position at a time. When the cursor reaches the bottom edge of the screen, it wraps around to the top.

Cursor Left - Moves the cursor left one position at a time. When the cursor reaches the left edge of the screen, it wraps round to the right edge and moves up one row. When it reaches the top left corner, it wraps round to the bottom right corner.

Cursor Right - Moves the cursor right one position at a time. When the cursor reaches the right edge of the screen, it wraps round to the left edge and moves down one row. When it reaches the bottom right corner, it wraps round to the top left corner.

Cursor Up - Moves the cursor up one position at a time. When the cursor reaches the top edge of the screen, it wraps around to the bottom.

Cut - Copies the marked area into the system clipboard and removes (clears) it from the display.

- If no area is marked, Cut clears the entire session window.

- Cut does not remove areas that are protected by the host application program.
- Cut does not remove host attributes such as color and intensity.

DBCS Input - Displays the DBCS character input window for a DBCS session. Type DBCS characters into the text field in this window. The text field allows you to invoke the country- or region-unique input method for entering DBCS characters. All other support key functions work from this window, so you don't need to close the window to perform other operations.

Delete Character - Deletes a character from an unprotected field.

The character at the cursor position is deleted and all characters to the right of the cursor (up to the last character of the same unprotected field) shift one position to the left. Null characters are inserted into the right-hand end of the field as the characters in the field are shifted left.

If you press this key when the cursor is not located in an unprotected field, X <-o-> (Go Elsewhere) appears in the operator information area.

Delete Word - Deletes the word under which the cursor is positioned and the following spaces or nulls, in an unprotected field. If the cursor is in the middle of the word (not on the first character), this function deletes the characters from the current cursor position to the end of the word, including the following spaces or nulls. All the words to the right of the deleted word (in the same field) shift to the left.

When you select this function and the cursor is not in an unprotected field, X <-o-> (Go Elsewhere) appears in the operator information area.

DUP Field - Places the DUP Field symbol on the screen and moves the cursor to the first position of the next unprotected field. Handling of the symbol is dependent on the application program.

The Dup character is usually displayed as overbar +*. However, due to a Java restriction, Host On-Demand displays Dup as *.

If you press this key and the cursor is not in an unprotected field, <-o-> (Go Elsewhere) appears in the operator information area.

End of Field (EOF) - Moves the cursor to the right of the last character in the same unprotected field.

Enter - When the host system is working on your application program or the session window is connected to a host system, Enter transmits data from the screen to the application program.

Enter or Reset - When the keyboard is locked, pressing this key resets the keyboard. When the keyboard is not locked, pressing this key transmits data from the screen to the application program.

Erase EOF - Erases all characters from the cursor position to the end of the field while the cursor is in an unprotected field. The erased characters are replaced with NULL. The cursor does not move. On an unformatted screen, this function erases all characters from the cursor position to the end of the screen. If you press this key when the cursor is not in an unprotected field, X <-o-> (Go Elsewhere) appears in the operator information area.

Erase Field - Erases all characters from the first position of the field to the end of the field while the cursor is in an unprotected field. The erased characters are replaced with NULL. The cursor moves to the first position in the field next to the field attribute. On an unformatted screen, this function moves the cursor to the top left corner of the screen and erases all characters from the cursor position to the end of the screen. If you select this function when the cursor is not in an unprotected field, X <-o-> (Go Elsewhere) appears in the operator information area.

Erase Input - Erases the contents of all input fields in the screen and moves the cursor to the beginning of the first unprotected field. If the screen has no unprotected field, the cursor moves to the top left corner; no data is erased. If the screen is unformatted, this function clears the screen and moves the cursor to the top left corner.

Field Exit - Signals the end of the field that has been entered. If it is a right-adjust field, right adjust is performed; the cursor is then positioned under the first input position of the next non-bypass input field.

Field Mark - Places the Field Mark symbol on the screen and the cursor moves to the next unprotected position. Handling of the symbol is dependent on the application program.

The Field Mark character is usually displayed as overbar +; . However, due to a Java restriction, Host On-Demand displays Field Mark as ; .

If you press this key when the cursor is not in an unprotected field, <-o-> (Go Elsewhere) appears in the operator information area.

Field Minus - Valid only in Signed Numeric and Numeric Only fields and functions identical to the Field Exit and Field Plus keys except for the following sign function.

In a Signed Numeric field, the F- key causes the reserved right-hand position to receive a minus sign. In a Numeric Only field, the low-order (units) digit is checked for a 0-9 numeric digit or a null character.

Field Plus - Signals the end of the field that has been entered. If it is a right-adjust field, right adjust is performed; the cursor is then positioned under the first input position of the next non-bypass input field. If this key is pressed on a signed numeric field, the sign position is set to null (displayed as a blank), indicating a positive field.

F1 through F24 - The program function keys provide a means of communicating with an application program. The program defines their usage.

Graphic cursor - Specifies whether the alphanumeric or the graphic cursor is active. When the graphic cursor mode indicator appears in the operator information area, the currently active cursor is the graphic. Absence of the indicator means the alphanumeric cursor is currently active.

Help - After an error condition, the operator uses this key to request that the host system send information about the error to the display.

Home - Moves the cursor to the first input-position of the screen. If the screen is unformatted, the cursor moves to the top left corner.

Insert - Toggles insert mode on or off. When the keyboard is in insert mode, the Insert symbol appears in the operator information area and the cursor changes to a half-block.

Insert allows you to insert a character into an existing unprotected field without writing over existing data. Null characters, displayed as blanks, must be in the right-most positions of the field where the insert will be performed.

When a new character is inserted at the cursor position, characters to the right of the cursor will shift one position to the right. If you attempt to insert characters even if there are no Nulls, X <-o-> (Go Elsewhere) appears in the operator information area. If the screen is unformatted or does not contain unprotected fields, Insert performs as if the whole screen were one field.

Jump Next Session - Changes the current session window to the next one that is not minimized.



Java Virtual Machines that do not support the WINDOW_ICONIFY and WINDOW_DEICONIFY events may not jump correctly if the session you are jumping to is, minimized.

New Line - Moves the cursor to the first input position in the next line.

If there are no input positions, the cursor moves to the top left corner of the screen. If the screen is unformatted, the cursor moves to the first character-position of the next line. If the cursor is in the last position of the screen, it wraps round to the first position.

Next Word - Moves the cursor to the first position of the next word that is in an unprotected field.

This function also performs an End of Field function: If the cursor is within the last word in a field, it is moved to the first position after that word if it is unprotected and before the end of the field.

When the cursor is not in the unprotected field, the cursor is moved to the first character of the first word in the next unprotected field.

If there isn't any words in any unprotected fields, the cursor is not moved.

PA1 through PA3 - The program attention keys provide a means of communicating with an application program. The

program defines their functions.

Page Down - Displays the next page.

Page Up - Displays the previous page.

Paste - Overlays the current contents of the system clipboard onto the session window, starting at the current cursor position.

- If the contents of the clipboard are larger than the space available in the presentation space (screen), it is clipped.
- Paste does not overlay the clipboard contents onto areas that are protected by the host application.

Previous Word - Moves the cursor to the first position of the previous word that is in an unprotected field. When the cursor is on a word in the unprotected field except the first position of the word, the cursor is moved to the first position on the word. When the cursor is not in the unprotected field, the cursor is moved to the first position on the last word of the previous unprotected field.

If there isn't any words in any unprotected fields, the cursor is not moved.

Reset - Reset has two functions:

1. Causes the session to leave insert mode and removes the insert symbol from the operator information area.
2. Unlocks the keyboard and removes the do-not-enter symbol X currently displayed in the OIA except in the Terminal Wait condition.

Rule - Rule line. Turns the rule line on or off (toggle).

SO/SI Display - Toggles the display of Shift Out characters (SO) and Shift In characters (SI) in a DBCS session.

System Request -

For 3270: Erases the screen and moves the cursor to the top left corner of the screen.

For 5250: Displays the system request menu. (Press Enter to display the menu.)

Tab Field - Moves the cursor from the current position to the first position of the next unprotected field. If there are no unprotected fields after the current cursor position, the cursor moves to the first character position of the first unprotected field on the screen. When the cursor is on the attribute character of the unprotected field, the cursor is moved to the first position in the field.

If the screen is unformatted or does not contain unprotected fields, Tab Field moves the cursor to the top left corner of the screen.

Tab Word - Moves the cursor to the first position of the next word.

Test Request - Sends a test request to the host system.

Related topics

- [Default keyboard mapping](#)
- [Remapping the Keyboard](#)
- [Bidirectional key definitions](#)

Custom Function Editor



The Custom Function Editor allows you to define and maintain custom functions without having to edit HTML and Java script files. Using the Custom Function Editor, you can add or delete a custom function. You can then go to the Keyboard Remap dialog, choose Custom Functions from the Category list, and your defined custom functions will appear in the list available for remapping. You can also assign a toolbar button to a custom function from the Keystroke page of the Customize Toolbar dialog.

To add a custom function:

1. Start from a host session window.
 - Click Edit > Preferences > Keyboard. From the Key Assignment tab, select the Custom Functions button.
or
 - Click Edit > Preferences > Toolbar > Add Button. From the Add Button panel, select the Keystroke tab and then select the Custom Functions button.
2. The Custom Function Editor dialog will be displayed.
3. Select Add to display the Add a Custom Function dialog.
4. Enter a name and data for the custom function (for example, you could specify to automate a logout by entering Logout in the Name field and logout[enter] in the Data field).

The Name value displays in the Keyboard Remap and Customize Toolbar function list box. The Data value is what the emulator processes when the remapped key or toolbar button is pressed.

See below for more information on the Data value.

5. Select OK.
6. After you have successfully assigned all the custom functions you want, select OK.

Selecting OK causes all data to be stored, and your defined custom functions will appear in the Custom Functions Category list on the Keyboard Remap and Customize Toolbar dialogs.

To delete a custom function:

1. Start from a host session window.
 - Click Edit > Preferences > Keyboard. From the Key Assignment tab, select the Custom Functions button.
or
 - Click Edit > Preferences > Toolbar > Add Button. From the Add Button panel, select the Keystroke tab and then select the Custom Functions button.
2. The Custom Function Editor dialog will be displayed.
3. Select a custom function from the Custom Function list, and select Delete. A Confirm Deletion dialog will appear.
4. Select OK.
5. After you have successfully deleted all the custom functions you want, select OK.

Selecting OK causes all data to be saved, and your selected custom functions will be deleted from the Custom Functions Category list on the Keyboard Remap and Customize Toolbar dialogs.

There are three rules to keep in mind when specifying the Data value.

- **Bracket encoding**

Host On-Demand supports the ability to process SendKeys mnemonics, so to send a bracket, you must use all double brackets `[[]]`. Single open and close brackets `[]` are translated as field boundaries for SendKeys mnemonics.

For more information about SendKeys, refer to Appendix A and the ECLPS class in the Host Access Class Library documentation.

- **Carat encoding**

The carat (^) is used to send characters that cannot be displayed. Place a ^ in front of any character with a value greater than or equal to A (hex 41, decimal 65) to translate to that value minus hex 40 or decimal 64; for example, "**^A**" = = hex 01, "**^B**" = = hex 02, and so on. The only way to get a ^ into the datastream is to double it. In other words, ^^ is equal to ^ in the datastream.

- **Unicode encoding**

You can use Unicode encoding to put displayable and non-displayable characters into the datastream. Unicode encoding uses the format **\uxxxx** where xxxx is two hex bytes. The value for the escape character is **\u001b**.

Related topics:

- [Remapping the keyboard](#)
- [Key Assignment](#)
- [Advanced Options](#)

Editing a macro



To edit a macro:

1. Click Macro Manager on the toolbar to display the Macro Manager toolbar.
2. Select a macro from the list.
3. Click Edit.
4. To edit the macro XML script directly, click Edit Code or use the Macro Editor. Use the Macro Editor to avoid introducing errors into the XML script.

Editing a macro using the Macro Editor

The Macro Editor separates a macro into four elements. Each tab represents an element:

[Macro](#)

Contains general information about the macro.

[Screens](#)

Contains all the screens defined in the macro and all descriptors and actions that are defined inside each screen.

[Links](#)

Defines the ordering of the screens.

[Variables](#)

Defines the macro variables.

Editing the XML script

Click Edit Code to edit the macro directly. The XML script for the current macro is displayed. Make any necessary changes to the code and click Save. The macro code is saved and the Macro Editor interface is updated. If errors are found, they are listed in the Messages section at the bottom of the window. Fix any problems before saving the macro. Click Cancel to return to the Macro Editor without saving any changes.

Importing a macro

Click Import to import a copy of a Host On-Demand macro from your workstation into the Macro Manager. You can import only Host On-Demand V3, Host On-Demand V4, Host On-Demand V5, and Host On-Demand V6 macros. When you import a macro and select Yes to replace the current macro, the current macro is saved and added to the macro list in the Macro Manager. The imported macro then becomes the current macro in the Macro Editor.

Exporting a macro

Click Export to copy a macro onto your workstation. This allows you to share the macro with other users.



Clicking Cancel discards all changes made since opening the Macro, not just for this tab. Clicking Save saves the entire Macro and closes the Macro Editor.

Related topics

- [Using the Macro Editor \(an overview\)](#)

- [Specifying a key as repeating or non-repeating](#)

Key repetition

Non-repeating keys


This box contains the keys that have been specified as non-repeating. In other words, these keys will not continue to generate letters or numbers automatically if you press them and do not release them immediately.

Add key

Click this button to add a key to the non-repeating key box.

Remove key

Click this button to remove a key from the non-repeating key box.


 The key-repeat function on Host On-Demand will not operate on machines using Linux or AIX. Consequently, you cannot map a key as "non-repeating" on a Linux or an AIX machine.

Specifying a key as repeating or non-repeating

Before you make any changes, all keys except for Ctrl, Alt, and Shift are set to repeat when you press them and keep them pressed. In other words, they continue to generate letters or numbers automatically if you press them and do not release them immediately. With this feature, you can specify whether a key repeats or not when you press it.

To change a key so that it does not repeat, complete the following:

1. Click Edit > Preference > Keyboard, or click the Remap button on the toolbar.
2. Click the Key Repetition tab.
3. Click Add a Key.
4. Press the key you want to change.

 The Ctrl, Alt, and Shift keys do not repeat and cannot be added to the list.


5. Click OK.

The key will then appear in the Non-repeating key box.

To change a key which was configured as non-repeating to repeating, complete the following:

1. In the Non-repeating keys box, click the key you want to change.
2. Click Remove Key.
3. Click OK.

The key will no longer appear in the Non-repeating key box.

 The key-repeat function on Host On-Demand will not operate on machines using Linux or AIX. Consequently, you cannot map a key as "non-repeating" on a Linux or an AIX machine.

Related topics:

- [Default characters and functions](#)
- [Remapping the keyboard](#)

Key repetition



Non-repeating keys

This box contains the keys that have been specified as non-repeating. In other words, these keys will not continue to generate letters or numbers automatically if you press them and do not release them immediately.

Add key

Click this button to add a key to the non-repeating key box.

Remove key

Click this button to remove a key from the non-repeating key box.



The key-repeat function on Host On-Demand will not operate on machines using Linux or AIX. Consequently, you cannot map a key as "non-repeating" on a Linux or an AIX machine.

Related topics:

- [Specifying a key as repeating or non-repeating](#)
- [Remapping the keyboard](#)



Server Connection Options

If you have selected the [Configuration server-based model](#) or the [Combined model](#) for your session configuration, use this panel to configure the client to use the [configuration servlet](#) or a different configuration server port.

By default, the Host On-Demand clients use port 8999 to access configuration information from the configuration server. If you are running [Host On-Demand through a 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. The configuration servlet tunnels the configuration information from the client to the configuration server over an HTTP or HTTPS connection using the defined configuration server port.

Using system defaults

Use system defaults will use the values specified in the [config.properties file](#) in the Host On-Demand publish directory. If you installed the configuration servlet or specified a different configuration server port as part of the Host On-Demand installation, the install program put the necessary parameters and values in *config.properties*. This file provides a global way of setting html parameters. All HOD applets request to read the *config.properties* file. If you choose Use system defaults, the values in the *config.properties* file for the configuration server port and the configuration servlet URL will be used by all HTML files.

Specifying a specific Configuration Servlet URL or a Configuration Server Port on this dialog will override any value in *config.properties*. If there are no values in *config.properties*, the client will contact the configuration server directly using port 8999.

Using the configuration servlet

If you don't want the client to use the system default values, uncheck Use system defaults, choose Yes to use the configuration servlet and specify the URL to where the [configuration servlet is installed](#). Check your web server or servlet engine's documentation for instructions on how to pass parameters to a servlet.

Changing the configuration server port

If you want the client to connect directly to the configuration server using a different port than the default or than is specified in the system defaults, uncheck Use system defaults, Choose No to using the configuration servlet, and specify the new port that the configuration server is listening on. You only need to change this from the default if you change what [the configuration server is listening on](#).

Printing directly from a host to a workstation printer (3270)

[Configuring printer sessions \(3270\)](#)

[Printer definition files \(3270\)](#)

[Printer definition tables \(3270\)](#)

[Compiling a printer definition table \(3270\)](#)

You can print host application files on a printer that is directly attached to your workstation or to a network printer.

On Windows platforms, Host On-Demand can use the native printer drivers provided by the workstation native operating system. On other platforms, Host On-Demand uses a **printer definition table (PDT)** to format data and send it to the printer as text and printer commands. A PDT can also be used on Windows platforms, but the native printer drivers on Windows platforms provide closer integration with the operating system. For example, you can choose a specific font used for print jobs.

PDTs provide great flexibility because you can customize them to produce the printed output you want without modifying the host application. PDTs also provide better printing performance than using the native printer drivers on Windows platforms. A PDT is customized by changing a **printer definition file (PDF)** and then compiling.

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. If you are working with a locally-installed client, the PDT is stored on the client workstation.

For more information, refer to the [Host Printing Reference](#).



A Host On-Demand 3270 printer session emulates an IBM 3287 printer in either LU Type 1 (SCS) or LU Type 3 mode. You do not have to specify which type of LU is supported by a particular session; the LU-type is configured at the host system and Host On-Demand detects the type automatically when the session is established.

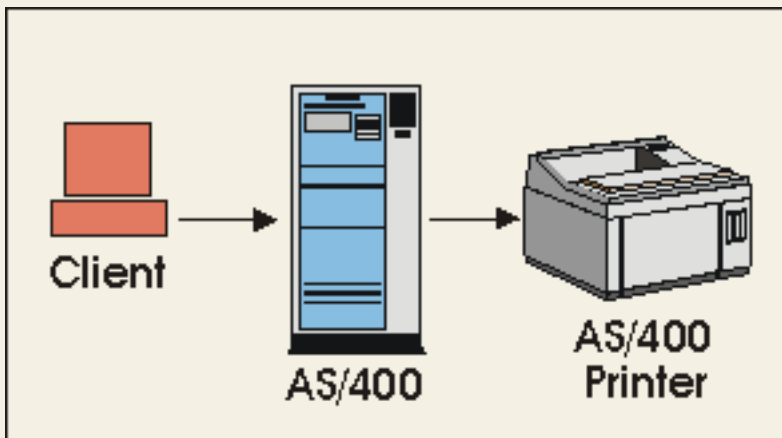
Printing directly from a host to a workstation printer (5250)

Host On-Demand provides the following functions for 5250 host printing:

- [Host Print key](#)
- [Host Print Transform](#)

Host print key (5250)

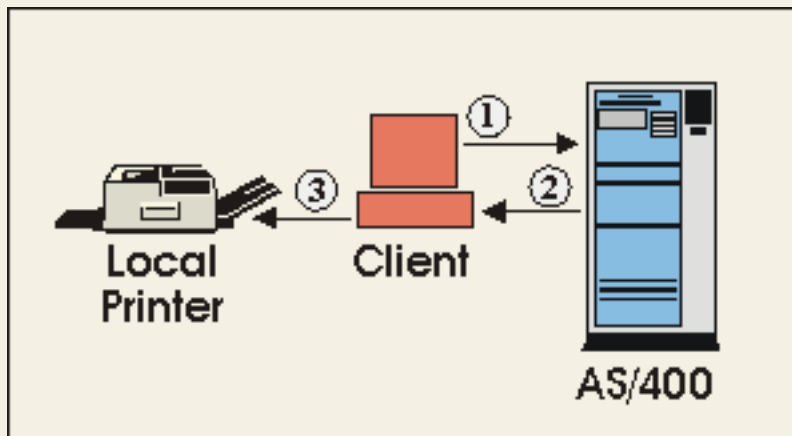
The Host Print key is available in a 5250 display session; it sends the contents of the presentation space to the iSeries as a print job that can be printed on any iSeries printer. If the job is directed to a Host On-Demand 5250 printer session, it will print on the printer specified for that session. The Host Print key is mapped by default to Ctrl-Pause.



Note: The Host Print key is not available for Screen Customizer sessions.

Host print transform (5250)

The 5250 host print transform function converts the iSeries print-data stream to ASCII just before it is sent from the iSeries to the PC printer. Having the conversion done on the iSeries ensures that most of the print processing is done there, not on the client.



1. The client session starts the host print transform to print a document.
2. The iSeries uses the host print transform to convert the print-data stream to ASCII, then sends the converted print-data stream back to the client.
3. The client prints the converted print-data stream on the locally attached print.

The ASCII print-data stream is suitable for many IBM and non-IBM printers; it uses iSeries system objects that describe the characteristics of a particular ASCII printer. When you configure a printer session, you just select the printer from the long list provided.

By default, Host On-Demand uses SCS-to-ASCII transform but you can configure the iSeries to do AFP-to-ASCII transform, which Host On-Demand also supports. The ASCII data stream is passed through the client by means of the SCS ASCII Transparency (ATRN) command; Host On-Demand deletes the command and passes the ASCII data stream to the workstation printer.

Related topics

- [Host Printing Reference](#)
- *iSeries Printer Device Programming Version 4* manual.



Compiling a printer definition table (3270)

Before you can compile a printer definition table (PDT), you must put a printer definition file (PDF) in the \pdfpdt\usrpdf\ subdirectory of the Web-published directory. The default Web-published directory is \hostondemand\hod.

A printer definition table is generated when a printer definition file that you have created or modified is compiled. To create a PDT:

1. Start the PDT compiler. On a Windows server or client, you can start the compiler through **Administration** on the **Start** menu. On other platforms, you must start it with a Java command. Sample command files are provided in the \lib\samples\CommandFiles\directory.
2. Select a [printer definition file](#) from the pull-down list.
3. Type a [description](#) for the printer definition table that you are going to create. A description is essential because it identifies the PDT when you configure a printer session.



The description must be unique.

4. Click OK. [Status and error information](#) appear at the bottom of the window; if there are errors in the PDF, correct them, and re-compile.

To compile other PDFs, repeat steps 1 through 4.

5. Click Exit when you have finished.

The compiler creates PDT (.hodpdt) files in the \pdfpdt subdirectory of the Web-published directory. When you run the compiler in graphical mode, it also creates a log, pdtc.log, which is overwritten each time you run the compiler. When you run the compiler in non-graphical mode, log output is sent to the screen, not to a file.

- [Printer definition table compiler \(3270\)](#)
- [Host Printing Reference](#)

Printer definition files (3270)

A Printer Definition File (PDF) is an ASCII file that contains macro definitions, session parameters, formatting controls, and character definitions. You can edit a PDF with an ASCII text editor to customize the file for the printer you will use. Most printers support similar commands for basic functions, but they differ widely in their support for more advanced functions.

Several PDFs are provided that should be suitable for most printers except those that use PostScript and the HP Printing Performance Architecture (PPA). PDFs from Communications Manager and Personal Communication can be compiled and used for Host On-Demand; however, not all controls in them are supported.

You can create a new PDF by typing the file or by customizing one of the IBM-supplied PDFs. In either case, you should use an ASCII editor; do not use a word-processing program. You cannot customize a PDT directly; you must modify one of the PDFs provided, or create a new one, and then compile it into a PDT. A compiler is provided.

The PDFs provided by IBM are installed in the \pdfpdt subdirectory of the Web-published directory. PDFs have the extension .pdf. A list of the PDF files and more information are included in the [Host Printing Reference](#).



If you want to customize one of the IBM-supplied PDFs to create your own, do not modify the original; copy it into the \pdfpdt\usrpdf\ subdirectory.

If you intend to create a customized PDT, you must have available the technical reference manual for the printer

concerned, so that you incorporate the correct control sequences into the PDF.

When you have modified or created a PDF, you must save it in the `\usrpdf` subdirectory of the `\pdfpdt` directory. You must create the directory the first time you do this.

Printer definition tables (3270)

A PDT is a file that is used to format the datastream sent by the host application. When a PDT is used, the Host On-Demand emulator converts the datastream from EBCDIC to ASCII (unless there is a `passthru` command in the datastream), formats the data according to controls specified in the datastream or in the PDT itself, and sends the data to the printer. You can use a simple PDT that contains basic instructions. However, if you want to use some of the functions that are available in modern workstation printers, such as the ability to change fonts or paper drawers, the PDT must be customized for the printer that you are using and the host application must send the necessary commands. You must, in any case, use a PDT that is suitable for the emulation mode that the printer supports (HP PCL Level 3, IBM PPDS, and so forth).

Several PDTs are provided with Host On-Demand for both Single-byte Character Set (SBCS) and Double-byte Character Set (DBCS) printers. You can create customized versions of these or entirely new ones. In either case, you will need a [printer definition file](#) from which to create a PDT.

The PDTs provided by IBM are installed in the `\pdfpdt` subdirectory of the Web-published directory. PDFs have the extension `.hodpdt`. A list of the files and more information is included in the [Host Printing Reference](#).

Printer definition table description (3270)

Every PDT must have a description, which serves to identify the PDT when you configure a printer session; the description must be unique. In graphical mode, the compiler checks that a unique description has been assigned. If the compiler finds that a PDT with the same description already exists, it stops compiling and displays an error message. You can change the description and click OK to start again.

The printer definition table compiler (3270)

The compiler is a Java application and therefore requires a Java runtime environment (jre). Host On-Demand installs a jre on a Windows server or client, but you must install it separately on other operating systems. You can run the compiler on a Host On-Demand server or locally-installed client, but not on a download client.

When you start the compiler in the usual way, it presents a graphical interface; this consists of two entry-fields (for a PDT name and a printer description) and a Status and Error Information window. The graphical interface is supported on all platforms.

You can also start the compiler in non-graphical mode by adding the PDT name and printer description as parameters of the command. The non-graphical mode is supported on all platforms.

Related topics

[Host Printing Reference](#)

Printer tab



The Printer tab window lets you choose the printer to be used with several related options.

[Print To \(3270/5250\)](#)

[Windows Printer \(3270/5250\)](#)

[Chose Windows Printer \(3270/5250\)](#)

[Windows Printer Name \(3270/5250\)](#)

[Select Printer \(3270/5250\)](#)

[Use Printer Definition Table \(3270\)](#)

[Print-to-File](#)

[Use Adobe PDF \(3270\)](#)

[Separate Files](#)

[View Every File in Browser](#)

[File Path and Name](#)

[Printer Definition Table \(3270\)](#)

[Printer Name](#)

[Printer Manufacturer \(5250\)](#)

[Printer Model \(5250\)](#)

[Paper Size \(source 1\) \(5250\)](#)

[Paper Size \(source 2\) \(5250\)](#)

[Envelope Size \(5250\)](#)

[ASCII Code Page 899 \(5250\)](#)

[Inactivity Time \(secs\) \(5250\)](#)

[Lock](#)

[Page Setup](#)

[Advanced Options \(3270\)](#)

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.

Chose Windows Printer (3270/5250)

Select Use Default to use the default Windows printer.

The default is Use Default.

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 PDF file. This is an option only if you select to print to a file.

The default value is No.

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 incremented 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.

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.



1. Most laser printers can use HP PCL Level 3. Level 3 commands are understood by later levels.
2. 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.
3. 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.
4. 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 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.

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.

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.

[Page Setup \(3270\)](#)**[Advanced Options \(3270\)](#)**

Status and error information (3270)



The bottom window of the graphical interface displays status and error information. Furthermore, when you use the graphical interface, a history of each compiler run is saved in the **pdtc.log** file (in the \usrpdf subdirectory). The log is overwritten each time you start the compiler.

In addition to verifying that the PDT description is unique, the compiler checks that the syntax of the PDF is correct and errors are displayed. Use an ASCII editor to correct the errors and compile the PDT again.

Advanced options (3270)

The Advanced Options window lets you choose several more advanced 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.

To return to the values that applied when the window was opened, click Cancel. To return to the default values, click Defaults.

- [Draw Field-Attribute Byte](#)
- [Printer-Font Code-Page](#)
- [Inactivity Time \(secs\)](#)
- [Concatenation Time](#)
- [Termination Time](#)
- [Best Fit](#)
- [Ignore Attributes](#)
- [SCS Sense-Code](#)
- [Inherit Parameters](#)
- [Tractor Feed](#)
- [Adobe PDF Options](#)
 - [Paper Size](#)
 - [Paper Orientation](#)
 - [Font](#)
- [Lock](#)

Draw Field-Attribute Byte

This option applies only to LU Type 3 sessions.

Use this option to determine how the 3270 field-attribute byte is drawn. Choose the None, Here, or Next options.

If you choose None, the field-attribute byte is drawn as a space character without an attribute.

If you choose Here, the field-attribute byte is used to draw the current byte. For example, if the current byte is defined as an underscore field, the field-attribute byte is drawn as a space character with the underscore attribute.

If you choose Next, the field-attribute byte is used to draw the next field-attribute byte.

The following illustrates each of the options:

```

axxxxxaxxxxxaxxxxx
|           |           |
|           |           | +-- Non-underlined field
|           |           | +-- Underlined field
+-- Underlined field
  
```

This is how each option prints:

a = field-attribute byte (prints as a blank)

none	here	next
axxxxxaxxxxxaxxxxx	axxxxxaxxxxxaxxxxx	axxxxxaxxxxxaxxxxx

Printer-Font Code-Page

When a PDT is being used, this parameter is useful only for printers that do not support the default code page. When a PDT is not being used on a Windows platform, this is useful for using a font that is not built as a Unicode font.

It defines the ASCII code page used for the font. When a PDT is being used, it should be consistent with the character code-points specified in the PDT file.

When a PDT is being used, the default is 850 for Latin-1 countries and regions, and the respective country or region's default ASCII code page for other countries or regions. When a PDT is not being used on a Windows platform, the default is Unicode.

Note: This option is not available if you are printing to an Adobe PDF file.

Inactivity Time (secs)

The inactivity time is used to monitor print jobs and pop up an 'intervention required' message if a printer error occurs. When a PDT is being used, the inactivity time can also be set by changing the INTERV_REQ_TIMER= session parameter in the PDT.

The default value is 10 seconds. A value of 0 disables the timer; a value below 11 sets an interval of 10 seconds; the maximum value is 255.

Note: This option is not available if you are printing to an Adobe PDF file.

Concatenation Time

If a value other than zero is specified for this field, that value is used as the expiration time for the print-job concatenation timer, which starts at the end of a print job. If the next print job arrives before the timer expires, that job is treated as a continuation of the previous job. If the time expires, an end-of-job command is sent to the printer and the next job is treated as a separate job.

The value is specified in seconds.

The default is zero, which means that the concatenation timer is not used (print jobs are never concatenated).

Note: This option is not available if you are printing to an Adobe PDF file.

Termination Time

If a value other than zero is specified for this field, that value is used as the expiration time for the print-job termination timer, which starts at the end of the print data. If another print-data record arrives before the timer expires, that job is treated as the continuation of the previous record. Otherwise, an end-of-job command is sent to the printer and the next print record is treated as the beginning of a separate print job.

The value is specified in seconds.

The default is zero, which means that print jobs are terminated by the end-of-job command but never by the timer.

Best Fit

This option is only available on Windows platforms when (1) Print to Windows Printer is selected and (2) a PDT is not being used.

If you select Yes, the Windows font size is calculated based on the Maximum lines per page and the Maximum characters per line options on the Page Setup tab (the Characters per inch and the Lines per inch options are ignored).

On LU Type 1 sessions, Host On-Demand ignores the Maximum lines per page, the Maximum characters per line, the Characters per inch, and the Lines per inch options that are set by SLD, SPD, SVF, or SHF SCS commands.

The default is No.

Note: This option is not available if you are printing to an Adobe PDF file.

Ignore Attributes

This option applies only to LU Type 3 sessions.

Choose Yes to ignore all 3270 attributes except non-printable attributes.

The default is No.

SCS Sense-Code

This option applies only to LU Type 1 sessions.

If you choose Yes, a negative response is sent to the host when an incorrect SCS command or parameter is received. If there is more data in the job, printing continues, although some of the printed data may be incorrect.

If you choose No, printing continues, but no notification is sent to the host. If there is a physical printer or connection problem, a sense-code is sent to the host even if you choose No.

The default is Yes.

Inherit Parameters

This option applies only to sessions using a PDT.

If you choose Yes, the parameters used in LU Type 1 print-job processing (such as, tab positions MPP or MPL) are inherited by the next job. This option is used when the host system sends a formatting command such as Set Horizontal Format for the first job, but assumes that the second and later jobs will use the format that is set for the first job.

The default is No.

Note: This option is not available if you are printing to an Adobe PDF file.

Tractor Feed

This option applies only to sessions using a PDT.

If you choose Yes, a form feed is not sent at the page boundary; a newline (NL) is sent instead. However, if a SET_AUTO_PERFORATION_SKIP command is defined in the PDT, a form feed is not sent, regardless of the setting of this option.

The default is No.

Note: This option is not available if you are printing to an Adobe PDF file.

Adobe PDF Options

This group box lists the options that are used in generating Adobe PDF files. These options are only available if you choose Print to File and Use Adobe PDF on the Printer tab.

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 depending 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).

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.

[Page Setup \(3270\)](#)

Page Setup tab (3270)



The Page Setup tab window 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 was not set to Yes on the Advanced Options window:

- Characters per inch
- Lines per inch
- Maximum lines per page
- Maximum characters per line

[Characters per inch](#)

[Lines per inch](#)

[Maximum lines per page](#)

[Maximum characters per line](#)

[Font](#)

[Select Font...](#)

[Suppress null lines](#)

[Print nulls as spaces](#)

[Suppress NL if CR at MPP+1](#)

[Suppress NL if NL at MPP+1](#)

[Ignore FF when at first position](#)

[FF takes space if before data](#)

[Form-feed position](#)

[Lock](#)

Characters per inch

Specifies the number of characters printed per inch. When a PDT is being used, the choices that appear are defined in the PDT. When a PDT is not being used on a Windows platform, three choices (10, 12, and 17) are available.

When a PDT is being used, the default value is taken from the DEFAULT_CPI? entry in the PDT, if this entry exists. When a PDT is not being used on a Windows platform, 10 is the default value.

Lines per inch

Specifies the number of lines per inch. When a PDT is being used, the choices that appear are defined in the PDT. When a PDT is not being used on a Windows platform, five choices (2, 3, 4, 6, and 8) are available.

When a PDT is being used, the default value is taken from the DEFAULT_LPI? entry in the PDT if this entry exists. When no PDT is being used on a Windows platform, 6 is the default value.

Maximum lines per page

Specifies the maximum number of lines per page, including the top and bottom margins. This value is also called Maximum Page Length (MPL). Enter a value from 1 to 255.

When a PDT is being used, the default value is taken from the MAXIMUM_PAGE_LENGTH entry in the PDT. If the entry is not found or when no PDT is being used on a Windows platform, the default value, 66, is used.

Maximum characters per line

Specifies the maximum number of characters per line and is also called the Maximum Print Position or the Maximum Presentation Position (MPP). Enter a value from 1 to 255.

When a PDT is being used, the default value is taken from the `MAXIMUM_PRINT_POSITION` entry in the PDT. If the entry is not found or when no PDT is being used on a Windows platform, the default value, 132, is used.

Font

This option only applies when a PDT is not being used on a Windows platform.

This field displays the currently-selected Windows font to be used for printing.

On Emulator clients (for example, `HOD.html`), this field is read-only. Click **Select Font** to change the font.

On Administration clients (for example, `HODAdmin.html`), you can type any font name in this field. Please be careful that the specified font is available on the client machines.

The default value varies depending on the current locale.

Select Font...

This option only applies when a PDT is not being used on a Windows platform.

Click this button to see the Font dialog window where you can specify a font to be used for printing.

Host On-Demand ignores the font style you select and uses a normal font style, except for intensified characters on LU Type 3 sessions, which print with a bold font style.

On single-byte character set 3270 printer sessions, Host On-Demand ignores the font size you specify. On double-byte character set 3270 printer sessions, Host On-Demand uses a 10 point font size if the character spacing is wide enough. If the character spacing is not wide enough, Host On-Demand calculates an appropriate point size based on the characters per inch and lines per inch.

You will not see a **Select Font** button on the Page Setup tab when running Host On-Demand on clients other than Windows.

Suppress null lines

This option applies only to an unformatted LU Type 3 job and when bits 2 and 3 in the Write Control Character (WCC) are not `B'00'`.

Choose **Yes** to suppress the lines that contain only non-printable characters; non-printable characters are nulls, characters in a non-print field, and field attributes. The space (blank) (`X'40'`) is considered a printable character.

Choose **No** to print a line that contains only non-printable characters as a blank line.

When a PDT is being used, the default value is taken from the `COMPRESS_LINE_SPACING?` entry in the PDT. If the entry is not found, or when a PDT is not being used on a Windows platform, the value **No** is used.

Print nulls as spaces

This option applies only to LU Type 3 sessions. Nulls are printed as spaces (`X'40'`).

When a PDT is being used, the default value is taken from the `OVERRIDE_FORMATTED_PRINT?` entry in the PDT. If the entry is not found, or when a PDT is not being used on a Windows platform, the value **Yes** is used.

Suppress NL if CR at MPP+1

This option applies only to an unformatted LU Type 3 job and when bits 2 and 3 in the Write Control Character (WCC) are `B'00'`.

Choose **Yes** to suppress an automatic-new-line if there is a Carriage Return (CR) code at (Maximum Print Position) `MPP+1`. For example, if the character 'A' is at `MPP` of line `n` and is followed by a CR code at `MPP+1` and the character 'B' at `MPP+2`, the 'A' is printed at the last position of line `n` and the 'B' is printed at the first position of the same line (overlapping).

Choose **No** to have 'B' print at the first position of line `n+1`.

When a PDT is being used, the default value is taken from the `NO_AUTO_NL_IF_CR_AT_MPP_PLUS_1?` entry in the PDT. If the entry is not found, or when a PDT is not being used on a Windows platform, the value **No** is used.

Suppress NL if NL at MPP+1

This option applies only to an unformatted LU Type 3 job and when bits 2 and 3 in the Write Control Character (WCC) are B'00'.

Choose Yes to suppress an automatic-new-line if there is a new-line (NL) code at MPP+1. For example, if the character 'A' is at MPP of line n and is followed by a NL code at MPP+1 and the character 'B' at MPP+2, the 'A' is printed at the last position of line n and the 'B' is printed at the first position of line n+1.

If you choose No, an NL at MPP+1 is effective after an automatic-new-line and the result is a blank line. For example, if the character 'A' is at MPP of line n and is followed by a NL code at MPP+1 and the character 'B' at MPP+2, the 'A' is printed at the last position of line n and 'B' is printed at the first position of line n+2.

When a PDT is being used, the default value is taken from the NO_AUTO_NL_IF_NL_AT_MPP_PLUS_1? entry in the PDT. If the entry is not found, or when a PDT is not being used on a Windows platform, the value No is used.

Ignore FF when at first position

If the session is LU Type 3 and you choose Yes, a form feed (FF) at the first position on the first line is ignored.

If the session is LU Type 1 and you choose Yes, an FF or a CR+FF combination at the beginning of a print job is ignored.

When a PDT is being used, the default value is taken from the IGNORE_FORM_FEED_AT_FIRST_POS? entry in the PDT. If the entry is not found, or when a PDT is not being used on a Windows platform, the value No is used.

FF takes space if before data

This option applies only to LU Type 3 sessions.

If you choose Yes, FF is executed, takes a print position, and is printed as a blank in the first position on the first line of the next page. Therefore, the next print-position will be the second position of that line.

If you choose No, FF is executed and the next print-position is the first position on the first line of the next page. That is, FF does not take a print position.

When a PDT is being used, the default value is taken from the FORM_FEED_TAKES_POSITION? entry in the PDT. If the entry is not found, or when a PDT is not being used on a Windows platform, the value Yes is used.

Form-feed position

This option applies only to LU Type 3 sessions.

If you choose the Any position option, FF is performed wherever it appears.

If you choose Column 1 only, FF is performed only if it appears at column 1. When FF is not at column 1, it is printed as a space character.

When a PDT is being used, the default value is taken from the FORM_FEED_ANY_POSITION? entry in the PDT. If this is defined as Any, any position is used. If the entry is not found, or when a PDT is not being used on a Windows platform, the value Column 1 only is used.

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 the tool bar can be changed.

[Advanced Options \(3270\)](#)

Running external commands after host print jobs



You can run external commands after each of your host print jobs have completed. On the Printer tab on the host printer session:

- Set the Print Destination to File.
- Set Separate Files to Yes.
This is necessary because an external command runs in a separate process. It is possible that a second print job could arrive before the external command completes execution, and if the print jobs are **not** saved as separate files, the arrival of the second print job may cause problems.
- Specify a File Path and Name, and any external commands.
File Path and Name must be valid for the operating system and the external commands must be valid commands for the operating system.

Windows example

On Windows platforms, you could specify: `c:\tmp\file.* | lpr -o 1 -S server -P printer $<`

where

- `c:\tmp\file.*` is the file that the print data is stored in. Host On-Demand numerically increments the file name for each print job. In this example, the first file will be named `file.000`, the next will be named `file.001`, and so on.
- the `|` sign separates the file name from external commands and their parameters;
- `lpr` is an external command;
- `-o 1 -S server -P printer` are parameters for the `lpr` command;
- and `$<` is converted to the file and path name by Host On-Demand. The command line that would be executed in this example looks like: `lpr -o 1 -S server -P printer c:\tmp\file.000`.

Linux example

On Linux, you could specify: `/home/user/file.* | lpr -b -Pprinter $<`

where

- `/home/user/file.*` is the file that the print data is stored in. Host On-Demand numerically increments the file name for each print job. In this example, the first file will be named `file.000`, the next will be named `file.001`, and so on.
- the `|` sign separates the file name from external commands and their parameters;
- `lpr` is an external command;
- `-Pprinter` are parameters for the `lpr` command;
- and `$<` is converted to the file and path name by Host On-Demand.



If the created file contains binary formatting instructions such as escape sequences, it is important to send the file to the printer in binary mode. Make sure to check the correct command syntax prior to usage.

- On Windows, this option is `-o 1` as in `lpr -o 1`.
- On Linux, this option is `-b` as in `lpr -b`.



Files are not erased even after the command execution has completed. You must either:

- Manually delete the files;
- Set the command to erase them. On Windows, the command line would look like this:

```
"c:\tmp\file.* | lpr -o l -S server -P printer $< && erase $<");
```

- Or create a batch file or shell script to print and delete the files, and specify the batch file or shell script as the external command in the File Path and Name field.

Availability of the lpr client software

The previous examples included the use of the lpr command. The lpr command allows you to send print jobs to printers shared by lpd if the lpr client software is installed.

The lpr client software is available on:

Unix (AIX, Linux, etc.), OS/2, and Windows 2000

The lpr client is usually installed by default.

Windows 95/98/Me

Microsoft does not provide the lpr client for Windows 95, 98 and Me. In order to use lpr, you must install third party lpr client software.

Windows NT 4.0

The lpr client software can be installed by installing the TCP/IP Printing services:

- Select Start > Settings > Control Panel and then double-click the Network icon
- Select the Services tab, and then click Add
- Select Microsoft TCP/IP Printing from the list of services, click OK, and click Close
- Shut down and restart your computer when prompted
- Reapply the latest Service Pack

The lpr command accepts different parameters on the various operating systems. Check the lpr documentation of your operating system for the appropriate parameters.

Printing from DOS to a PPA printer (HP Desk Jet 700 series)

By configuring an external command to run after print jobs, you can also print to a PPA printer (for example, the HP Desk Jet 700 series) from DOS. This procedure works for Windows NT 4.0, Windows 95 and 98, whether you are directly connected to the printer or printing to a shared PPA printer with net use. You need to disable bidirectional communication and the launch Toolbox when printing features from the printer's configuration menu by following these steps:

1. Click Start > Run.
2. Type HPFCFG14 and click OK. If HPFCFG14 does not work, try either HPFCFG06 or HPFCFG13.

3. In the HP DeskJet Configuration dialog box, click Continue.
4. Click on Bidirectional Communication and Launch Toolbox When Printing to clear these options, then click OK.
5. Click Return to Windows.
6. Click Start > Run.
7. Type HPFDJC14.INI and click OK. If your system cannot find HPFDJC14.INI, try either HPFDJC06.INI or HPFDJC13.INI.
8. If you have the version 10.3 driver in the HP DeskJet 700 series, change the `DSMEnable` parameter from either `DSMEnable=0100` or `DSMEnable=0200` to `DSMEnable=0000`.
9. Click File and Save
10. Exit and restart Windows.

Now print the files using the Copy command to lpt1. For example, `copy file.prt lpt1`

Transferring files

Host On-Demand allows you to transfer files between a client and a host in a number of ways:

Using Host File Transfer to transfer files

1. Start a host session.
2. Make sure that the correct [host system and other options](#) have been specified.
3. Click Transfer Files > Send or Receive, or the Send or Recv button on the toolbar.



When sending a file to an MVS/TSO host partitioned data set, the data set must already exist on the host.

4. Fill in the names of the PC and host files. You can click Browse to find a PC file or an OS/400 file. When you click in the box for the target file, Host On-Demand automatically generates a filename. If you want to transfer an existing list of files, click Open List and choose the list.
5. Set the [transfer](#) mode.
6. If you want to change any of the [transfer options](#) (parameters), click Options. The change applies only to the file that is currently in the Add File to Transfer List box.
7. Click Add to List. The file names and transfer mode appear in the list box.
8. If you want to transfer several files, repeat steps 4 - 7.
9. To transfer the files in the list, click Send or Receive.
10. To save the list, click Save List and enter a name for the list.



A list can be used only for the purpose for which it was created. You cannot use a send list to receive files and you cannot use a list created for MVS/TSO for VM/CMS transfers. That is because options are often specific to host type and direction of transfer.

Using an FTP session to transfer files

1. Start an FTP session.
2. Click on the file or directory you want to transfer. If you do not see the file or directory you want to transfer, you can use the working directory field above each of the file systems to change to the directory that contains the files or directories you want to transfer, or to change to the directory that you want to transfer files or directories into, by typing the fully qualified path.
3. Click the arrow button in between the local file system and the remote file system to transfer the file or directory.

Using a host session configured to use FTP to transfer files

1. Start a host session.
2. Select Actions > Transfer Files. Login to the FTP server if you are prompted to do so when the FTP session displays .
3. Select the file or directories you want to transfer. If you do not see the files or directories you want to transfer, you can use the working directory field above each of the file systems to change to the directory that contains the files or directories you want to transfer, or to change to the directory that you want to transfer files or directories into, by typing the fully qualified path.
4. Click the arrow button in between the local file system and the remote file system to transfer the files or directories.

Related topics:

- [File Transfer overview](#)
- [FTP client overview](#)

Setting file transfer default options



You can change the file transfer default options for both Host File Transfer and FTP File Transfer.

Setting host file transfer default options

Each host system has its own transfer options.

- [General](#)
- [MVS/TSO](#)
- [VM/CMS](#)
- [CICS](#)
- [OS/400](#)

You can get to the host file transfer default options by:

- From a session configuration window, as a user or as an administrator: open the session properties and click File Transfer.
- From a session itself: click Actions > File Transfer Defaults, or click Edit > Preferences > File Transfer Defaults.

Then do as follows:

- On the General tab, set the correct host system for this session. If the host system is incorrect, transfer will fail because the wrong options are used. Change the other parameters as necessary.
- To change any of the file transfer options, click the tab for the appropriate host system. For OS/400, VM/CMS and CICS, the first option must be preceded by an open parenthesis '('.
- Click OK when you finish.

Setting FTP default file transfer options

You can set a number of FTP transfer options.

- [Connection tab](#)
- [Advanced tab](#)
- [More Advanced tab](#)
- [Screen tab](#)

You can get to the FTP file transfer default options by:

- From the Client window, as a user or as an administrator: right-click on the session to open and click Properties.
- From the Administrator window, right-click on the user or group and select Sessions. Right-click on the FTP session in the Configured Sessions window and select Properties.
- From a session itself, configured to use FTP for file transfer instead of host file transfer: click Actions > File Transfer Defaults, or click Edit > Preferences > File Transfer Defaults.

Then do as follows:

- On the Connection tab, set the Destination Address, User ID and Password for this session. Change the other parameters as necessary.

- On the Advanced tab set the ASCII File Types list and any other applicable parameters.
- Click OK when you finish.

Default transfer mode



Options include:

TEXT

This option sets the default transfer mode to be Text (for text only files).

BINARY

This option sets the default transfer mode to be Binary. Binary files are files stored as a series of numbers and symbols that only computers can read. Applications and pictures are examples of binary files.

File transfer overview



Host On-Demand provides two ways to transfer files between a client and a host:

Host File Transfer

- You can transfer files between your workstation and zSeries systems running MVS/TSO, VM/CMS or MVS/CICS. You can also transfer files between your workstation and the Integrated File System (IFS) of OS/400 V3R7 or later.

For zSeries, file transfer uses the IND\$FILE (SBCS) or APVUFILE (DBCS) program; for iSeries, no extra software is required.
- The Host On-Demand interface is the same in all cases except that, for OS/400, there is a button that lets you browse the IFS.
- You can transfer a single file or a list of files and you can save the list for repeated use. You can also modify and delete lists. The same interface is used in all cases.
- File transfer will work only if the host system screen has a command line available. Please refer to [Planning, Installing, and Configuring Host On-Demand](#) for details.
- For 5250 file transfer on Netscape 4.x, you cannot connect to a V5R1 iSeries host that has long password support enabled. The Netscape 4.x JVM does not implement the APIs required to encrypt long passwords. You can use a different browser or install the Netscape 4.x Java 2 plug-in.
- In order make iSeries file browsing more efficient when browsing files under the QSYS library, Host On-Demand only lists the files that can be transferred under the QSYS library file system. This may change your file list when you browse the QSYS file system. Host On-Demand lists:
 1. only * .LIB objects as directories under the QSYS library.
 2. objects under * .FILE as files under the QSYS library.
 3. only * .FILE objects as directories under any other library.

File Transfer Protocol (FTP)

- You can transfer files or directories between your workstation and any host system running an FTP server. Host On-Demand implements the client functionality specified by File Transfer Protocol (FTP), which is the standard protocol for transferring files to and from remote machines running FTP servers.
- You can configure 3270, 5250 and VT sessions to use the FTP client as the default file transfer type, instead of Host File Transfer. The FTP session starts in a separate browser window from the host session. The FTP client interface is the same in all cases.
- You can transfer, delete and rename a single file or directory or multiple files or directories from either the local file system or the remote file system.

Related topics:

- [Transferring files](#)
- [Changing a file transfer list](#)
- [Setting default transfer options](#)

FTP client overview



Host On-Demand implements the client functionality specified by File Transfer Protocol (FTP), which is the standard protocol for transferring files to and from remote machines running FTP servers. The FTP client allows file and directory upload, file and directory download, and directory navigation of remote and local file systems.

You can use the FTP client in two ways: you can configure stand-alone FTP sessions, and you can configure a 3270, 5250, or a VT session to use FTP as the default file transfer type instead of Host File Transfer. When you configure a stand-alone FTP session, an FTP session icon is added to the Host On-Demand Client window and is started the same way as you start other sessions. When you configure a 3270, 5250 or a VT session to use FTP as the default file transfer type, the FTP session starts in a separate browser window. Once it starts, the FTP session is displayed in the Active Sessions area of the Host On-Demand Client window indicating current connection status. If you use a secure host session configured to use FTP to transfer files, the FTP client session is not secure.

The FTP client implements RFC2640, which addresses the Internationalization (I18n) of the File Transfer Protocol to support multiple character sets and languages. RFC2640 enhances the capabilities of the File Transfer Protocol by removing the 7-bit restrictions on path names used in client commands and server responses, and defines a new command for language negotiations. The RFC recommends the use of the UTF-8 encoding format. UTF-8 is a UCS (Universal Character Set ISO/IEC 10646 [ISO-10646]) transformation format (UTF). It is a safe file encoding that avoids the use of byte values that have special significance during the parsing of path name character strings.

The RFC also defines a new command, LANG, that negotiates a language for greetings and error messages exchanged between FTP servers and clients. Once the server and the FTP client successfully negotiate a language, the server must return server messages and command response text in the negotiated language and encoded in UTF-8. The LANG command affects only greetings and command response text. Any greetings and command response text before the server and the FTP client negotiate a language appear in the server's default language. If the FTP server does not support the LANG command or the language being negotiated by the FTP client, then the server greetings and responses appear in ASCII US-English. If the FTP server does not support UTF-8 encoded path names, then path names are encoded in 7-bit ASCII.



The UTF-8 encoding format applies only to path names and not to the contents of a file. The encoding scheme of a file depends on the local operating system.

The FTP client provides access to internet FTP servers through a firewall. When the FTP client within a firewall detects that the FTP server is outside the firewall, passive mode (PASV) is automatically activated, which allows the FTP client to access the FTP server through the firewall.

The FTP client does not replace the existing Host File Transfer function. See [File transfer overview](#) for more information about the differences between FTP File Transfer and Host File Transfer.

Notes and Limitations:

- FTP is not a secure protocol, so the FTP client cannot be used with SSL. If you use a secure host session configured to use FTP to transfer files, the FTP client session is not secure.
- Screen Customizer does not support the FTP client, so if the Screen Customizer session property is enabled in a display session's properties then the supported File Transfer Type is Host File Transfer, not FTP.
- The FTP client does not support the drag-and-drop GUI function.
- Directory transfer is not supported on systems that do not have directory structures similar to Windows and Unix, for example, VM, OS/390 or z/OS MVS services, OpenVMS, and OS/400 Library File System.
- The local file list does not support listing multiple local or LAN-attached drives. To view files on a different drive, type the drive letter of the drive you would like to view in the Directory field and press the Enter key. The new drive is displayed in the local file list. You must set the Local Home Directory parameter in the session configuration dialog in order to permanently change the local drive or directory.
- When you configure a 3270, 5250, or VT session to use FTP as the default file transfer type instead of Host File Transfer, some changes to FTP session properties are not saved. The following settings are not saved:

- Window size and position
 - Visibility of Toolbar, Toolbar Text, Status Bar and Transfer List Manager
 - Any changes to the Toolbar
 - Confirm On Exit
- When an FTP session is used to connect to a server outside the firewall on a socksified Host On-Demand client (the browser is configured to communicate through a socks server), the connection might fail. The FTP session may hang.

To correct this problem, log off Host On-Demand, and restart the browser. Select Passive for the Data Connection Mode on the More Advanced tab and restart the session.

- When you establish a Host On-Demand FTP session with a Microsoft FTP Server, download a file, and then delete the file on the remote system, the deleted file still appears in the file list on the remote system. If you refresh the remote file list several times, the deleted file disappears. The FTP server appears to not close the file descriptor of the deleted file after you delete it. Therefore, the operating system does not get rid of the file immediately.
- On Windows 95, Windows NT, and Windows 2000 running Netscape 4.79 or earlier, you cannot view the first logical file on the floppy drive (A:\). When the floppy is blank, the Java File.list() command that retrieves the file listing returns null. The FTP client always returns one less file than actually on the disk.
- On Windows 2000 and a NTFS local file system, some of the hidden files, for example, AUTOEXEC.BAT, do not appear in the local directory listing on Netscape. The Java File object does not provide these files to the FTP client.

Related topics

- [FTP client session window](#)

General options



The general settings for each host type include:

Host Type

The type of host to which this session will connect. This determines which set of default options are used.

Timeout (in seconds)

This option specifies the length of time (in seconds) that the workstation waits for a response from the host. Only numeric characters 0-9 are allowed. The acceptable range is from 20 to 65535 or 0: (if you specify 0, a timeout will not be set). The default is 30.

If the host does not respond within this time, the file transfer is canceled, and you receive an error message. You might need to increase the value if you have a slow connection.

PC Code-Page

The code-page is a table that translates EBCDIC codes to PC 1-byte codes, or vice versa, when files are transferred.

The default corresponds to the host code-page that was set in the session configuration.

Pause

The number of seconds to pause between each transfer.

File Transfer User ID

You must log on to an OS/400, specifically to do file transfer, even if you are already logged on to a display or printer session. The user ID that is specified here will be used to pre-fill the user ID field in the logon window when you initiate a file transfer.

File Transfer Destination Address

This option specifies the actual final destination address of the host to be used for the file transfer.

Enable Proxy Server

Enables you to use a OS/400 proxy server during the file transfer. The OS/400 proxy server service is started by the Host On-Demand server.

The default is No.

Proxy Server Destination Address

Specifies the address of the OS/400 proxy server, which is started by the Host On-Demand Server, to be used for the file transfer. It is used only when the Proxy Server is enabled.

Proxy Server Destination Port

Specifies the port number of the OS/400 proxy server to be used for the file transfer. It is used only when the Proxy Server is enabled.

The default is 3470.

Host-File Orientation

This option applies if the session is configured for an Arabic or Hebrew host code-page and specifies whether the host files you transfer will be saved, in left-to-right or right-to-left format.

The default is Left-to-Right.

PC-File Orientation

This option applies if the session is configured for an Arabic or Hebrew host code-page and specifies whether the PC files you transfer will be saved, in left-to-right or right-to-left format.

The default is Left-to-Right.

PC-File Type

This option applies if the session is configured for an Arabic or Hebrew host code-page and specifies whether the PC files you transfer will be saved, in the format in which they are saved (Implicit) or in the format in which they should be displayed.

The default is Implicit.

Lam-Alef Expansion

This option applies if the session is configured for an Arabic host code-page. When receiving files from the host, the character *Lam_alef* is expanded into two characters, *Lam* followed by *Alef*. This option is available for Windows PC code-page 1256 and AIX ISO code-page 1089.

The default is to do expansion.

Lam-Alef Compression

This option applies if the session is configured for an Arabic host code-page. When sending files to the host, the characters *Lam* followed by *Alef* are compressed into one character, *Lam_alef*. This option is available for Windows PC code-page 1256 and AIX ISO code-page 1089.

The default is to do compression.

MVS/TSO options

- [Send text options](#)
- [Receive text options](#)
- [Send binary options](#)
- [Receive binary options](#)
- [Default transfer mode](#)
- [Clear before Transfer](#)

Send text options (MVS/TSO and VM/CMS)



The following options are used (by default) when sending files in text mode. For VM/CMS, remember to type an open parenthesis '(' before the first option.

Options include:

ASCII

Use this option for text files and for files that you want to be converted from ASCII to EBCDIC. This is valid for SBCS languages, Traditional Chinese, and Korean. PC 1-byte codes are converted into EBCDIC codes. For DBCS, inserts shift in/shift out (SI/SO) characters into DBCS fields.

JISCII

This option is valid for Japanese DBCS sessions only and converts 1-byte codes to EBCDIC and 2-byte codes to IBM Kanji. JISCII inserts shift in/shift out (SI/SO) characters into DBCS fields.

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is removed from the end of each line. EOF (x'1A') is removed from the end of a file.

NOSO

This option is valid only for DBCS and only when used with the JISCII or ASCII option. NOSO prevents the conversion of SO (x'0E') and SI (x'0F') before and after the DBCS field. It also prevents the conversion of RS (x'1E') and US (x'1F') to SO (x'0E') and SI (x'0F').

APPEND

The transferred file will be appended to an existing host file that has the same name (and type and mode for VM/CMS), if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

LRECL

Logical Record Length. This is not valid if APPEND is specified. Otherwise, you can choose one of the following options:

- Fixed - Specifies the number of bytes in each host record.
- Variable - The logical record length is the length of the longest record in the file; the maximum value is 32767.

The record length of a file sent from a PC to the host system might exceed the logical record length specified here. If so, the file transfer program divides the file by the logical record length.

To send a file containing long records to the host system, specify a length that is long enough to allow complete records to be sent.

RECFM

Record Format. This option is not valid when APPEND is specified. Otherwise, you can choose one of the following options:

- Default - The record format is automatically selected by the host system.
- Fixed - Specifies the number of bytes in each host record.
- Variable - When sending a file to VM/CMS, you can conserve host disk space by specifying a record format of variable.
- Undefined - This option is available for MVS/TSO only.

BLKSIZE(n)

This option applies only to TSO and only when you are creating a new data set. The (n) value represents the block size in bytes.

SPACE

This option applies to TSO only. This value is the amount of space to be allocated for a new TSO data set.

Quantity

Units of space to be allocated initially. You must specify this value when the SPACE parameter is used.

Increment

Units of space to be added each time new space is required.

The following parameters are only valid when the SPACE parameter is specified, and are mutually exclusive of each other.

AVBLOCK(n)

Average block length used as the unit size by the SPACE parameter. The (n) value is the block length in bytes.

TRACKS

Specifies the unit of space is a track.

CYLINDERS

Specifies the unit of space is a cylinder.

UNICODE (encoding)

This option is only for DBCS code pages. It allows you to send text files saved in UNICODE to the host and convert them to EBCDIC. Valid encoding options are UCS2 or UTF8. The default encoding option UCS2 is used if neither option is specified. The UTF-8 encoding option is the same as UTF8.

Receive text options (MVS/TSO and VM/CMS)



The following options are used (by default) when receiving files in text mode. For VM/CMS, remember to type an open parenthesis '(' before the first option.

Options include:

ASCII

Use this option for text files and for files that you want to be converted from EBCDIC to ASCII. This is valid for SBCS languages, Traditional Chinese, and Korean. EBCDIC codes are converted to PC 1-byte codes. For DBCS, removes shift out/shift in SO/SI characters from DBCS fields.

JISCII

This option is valid for Japanese DBCS sessions only and converts EBCDIC code to 1-byte codes and 2-byte codes to IBM Kanji. JISCII removes shift out/shift in (SO/SI) characters from DBCS fields.

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is added at the end of each line. EOF (x'1A') is added at the end of the file. If APPEND is specified, EOF is removed from the end of an existing file and is added at the end of an appended file.

SO

This option is valid only for DBCS and only when used with the JISCII or ASCII option. It allows the conversion of SO (x'0E') and SI (x'0F') to RS (x'1E') and US (x'1F').

USER

This option is valid only for DBCS and only when used with the ASCII (JISCII) and SO options. If USER is specified, SO (x'0E') and SI (x'0F') will not be converted to RS(x'1E') and US(x'1F').

APPEND

The transferred file will be appended to an existing PC file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing PC file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

UNICODE (encoding)

This option is only for DBCS code pages. It allows you to receive text files saved in EBCDIC from the host and convert them to UNICODE. Valid encoding options are UCS2 or UTF8. The default encoding option UCS2 is used if neither option is specified. The UTF-8 encoding option is the same as UTF8.

Send binary options (MVS/TSO and VM/CMS)



Options include:

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is removed from the end of each record. EOF (x'1A') is removed from the end of a file.

APPEND

The transferred file will be appended to an existing host file that has the same name (and type and mode for VM/CMS), if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

LRECL

Logical Record Length. This is not valid if APPEND is specified. Otherwise, you can choose one of the following options:

- Fixed - Specifies the number of bytes in each host record.
- Variable - The logical record length is the length of the longest record in the file; the maximum value is 32767.

The record length of a file sent from a PC to the host system might exceed the logical record length specified here. If so, the file transfer program divides the file by the logical record length.

To send a file containing long records to the host system, specify a length that is long enough to allow complete records to be sent.

RECFM

Record Format. This option is not valid when APPEND is specified. Otherwise, you can choose one of the following options:

- Default - The record format is automatically selected by the host system.
- Fixed - Specifies the number of bytes in each host record.
- Variable - When sending a file to VM/CMS, you can conserve host disk space by specifying a record format of variable.
- Undefined - This option is available for MVS/TSO only.

BLKSIZE(n)

This option applies only to TSO and only when you are creating a new data set. The (n) value represents the block size in bytes.

SPACE

This option applies to TSO only. This value is the amount of space to be allocated for a new TSO data set.

Quantity

Units of space to be allocated initially. You must specify this value when the SPACE parameter is used.

Increment

Units of space to be added each time new space is required.

The following parameters are only valid when the SPACE parameter is specified, and are mutually exclusive of each other.

AVBLOCK(n)

Average block length used as the unit size by the SPACE parameter. The (n) value is the block length in bytes.

TRACKS

Specifies the unit of space is a track.

CYLINDERS

Specifies the unit of space is a cylinder.

Receive binary options (MVS/TSO and VM/CMS)



Options include:

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is added at the end of each record. EOF (x'1A') is added at the end of the file. If APPEND is specified, EOF is removed from the end of an existing file and is added at the end of an appended file.

APPEND

The transferred file will be appended to an existing PC file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

Clear before transfer



This option sends a Clear Presentation Space command before transferring a file. You should not change this setting unless you have a good reason because in nearly every case, CMS and CICS require that this command be sent, whereas TSO and OS/400 do not.

VM/CMS options

- [Send text options](#)
- [Receive text options](#)
- [Send binary options](#)
- [Receive binary options](#)
- [Default transfer mode](#)
- [Clear before Transfer](#)

CICS options

- [Send text options](#)
- [Receive text options](#)
- [Send binary options](#)
- [Receive binary options](#)
- [Default transfer mode](#)
- [Clear before Transfer](#)

Send text options (CICS)



Options include:

ASCII

Use this option for text files and for files that you want to be converted from ASCII to EBCDIC. This is valid for SBCS languages, Traditional Chinese, and Korean. PC 1-byte codes are converted into EBCDIC codes. For DBCS, inserts shift in/shift out (SI/SO) characters into DBCS fields.

JISCII

This option is valid for Japanese DBCS sessions only and converts 1-byte codes to EBCDIC and 2-byte codes to IBM Kanji. JISCII inserts shift in/shift out (SI/SO) characters into DBCS fields.

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is removed from the end of each line. EOF (x'1A') is removed from the end of a file.

NOSO

This option is valid only for DBCS and only when used with the JISCII or ASCII option. NOSO prevents the conversion of SO (x'0E') and SI (x'0F') before and after the DBCS field. It also prevents the conversion of RS (x'1E') and US (x'1F') to SO (x'0E') and SI (x'0F').

APPEND

The transferred file will be appended to an existing host file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

Receive text options (CICS)



You can only receive one file at a time during CICS file transfer.

Options include:

ASCII

Use this option for text files and for files that you want to be converted from EBCDIC to ASCII. This is valid for SBCS languages, Traditional Chinese, and Korean. EBCDIC codes are converted to PC 1-byte codes. For DBCS, removes shift out/shift in (SO/SI) characters from DBCS fields.

JISCII

This option is valid for Japanese DBCS sessions only and converts EBCDIC code to 1-byte codes and 2-byte codes to IBM Kanji. JISCII removes shift out/shift in (SO/SI) characters from DBCS fields.

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is added at the end of each line. EOF (x'1A') is added at the end of the file. If APPEND is specified, EOF is removed from the end of an existing file and is added at the end of an appended file.

SO

This option is valid only for DBCS and only when used with the JISCII or ASCII option. It allows the conversion of SO (x'0E') and SI (x'0F') to RS (x'1E') and US (x'1F').

APPEND

The transferred file will be appended to an existing PC file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing PC file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

Send binary options (CICS)



Options include:

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is removed from the end of each record. EOF (x'1A') is removed from the end of a file.

APPEND

The transferred file will be appended to an existing host file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

Receive binary options (CICS)



You can only receive one file at a time during CICS file transfer.

Options include:

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is added at the end of each record. EOF (x'1A') is added at the end of the file. If APPEND is specified, EOF is removed from the end of an existing file and is added at the end of an appended file.

APPEND

The transferred file will be appended to an existing PC file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

OS/400 options

- [Send text options](#)
- [Receive text options](#)
- [Send binary options](#)
- [Receive binary options](#)
- [Default transfer mode](#)

Send text options (OS/400)



Options include:

ASCII

Use this option for text files and for files that you want to be converted from ASCII to EBCDIC. This is valid for SBCS languages, Traditional Chinese, and Korean. PC 1-byte codes are converted into EBCDIC codes. For DBCS, inserts shift in/shift out (SI/SO) characters into DBCS fields.

JISCII

This option is valid for Japanese DBCS sessions only and converts 1-byte codes to EBCDIC and 2-byte codes to IBM Kanji. JISCII inserts shift in/shift out (SI/SO) characters into DBCS fields.

UNICODE (encoding)

This option lets you send text files (saved in UNICODE) to the host and converts the data from UNICODE to EBCDIC. You can specify either UCS2 or UTF8 as the encoding option. If neither is specified, the default, UCS2, is used.

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is removed from the end of each line. EOF (x'1A') is removed from the end of a file.

NOSO

This option is valid only for DBCS and only when used with the JISCII or ASCII option. NOSO prevents the conversion of SO (x'0E') and SI (x'0F') before and after the DBCS field. It also prevents the conversion of RS (x'1E') and US (x'1F') to SO (x'0E') and SI (x'0F').

APPEND

The transferred file will be appended to an existing host file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

DSTADDR(dstaddr)

This option specifies the destination address of the host to be used for the file transfer.

USERID(usr)

This option specifies the user ID to be used for the file transfer.

PASSWORD(pwd)

This option specifies the password to be used for the file transfer.

SRC

This option specifies the OS/400 file type to be used for the transfer. If the host file does not exist, then a new file is created with the file type "Source physical file". This option is applicable only for the files in the QSYS library file system.

DTA

This option specifies the OS/400 file type to be used for the transfer. If the host file does not exist, then a new file is created with the file type "Physical data file". This option is applicable only for the files in the QSYS library file system.

LRECL(n)

This option specifies the logical record length when creating a file on the OS/400. It can have the following values:

- An integer from 1 through 32766 when **Host File Type** is set to **Source physical file**.
- An integer from 1 through 32754 when **Host File Type** is set to **Physical data file**.
- It is ignored when **Host File Type** is set to **Save file**.



Microsoft Internet Explorer users may see this error message in the java console while transferring files to the OS/400:

```
com.ms.SecurityExceptionEx[com/ibm/as400/access/SystemProperties/GetProperty]:  
Unable to access system property: com.ibm.as400.Trace.category
```

This message can be ignored. If you want to remove the error message from the java console you can update the Windows registry entry

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM\classpath
```

with the Host On-Demand server directory, for example *c:\hostondemand\hod*.

Receive text options (OS/400)



Options include:

ASCII

Use this option for text files and for files that you want to be converted from EBCDIC to ASCII. This is valid for SBCS languages, Traditional Chinese, and Korean. EBCDIC codes are converted to PC 1-byte codes. For DBCS, removes shift out/shift in SO/SI characters from DBCS fields.

JISCII

This option is valid for Japanese DBCS sessions only and converts EBCDIC code to 1-byte codes and IBM Kanji to 2-byte codes. JISCII removes shift out/shift in (SO/SI) characters from DBCS fields.

UNICODE (encoding)

This option lets you receive text files (saved in EBCDIC) from the host and converts the data from EBCDIC to UNICODE. You can specify either UCS2 or UTF8 as the encoding option. If neither is specified, the default, UCS2, is used.

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is added at the end of each line. EOF (x'1A') is added at the end of the file. If APPEND is specified, EOF is removed from the end of an existing file and is added at the end of an appended file.

SO

This option is valid only for DBCS and only when used with the JISCII or ASCII option. It allows the conversion of SO (x'0E') and SI (x'0F') to RS (x'1E') and US (x'1F').

USER

This option is valid only for DBCS and only when used with the ASCII (JISCII) and SO options. If USER is specified, SO (x'0E') and SI (x'0F') will not be converted to RS(x'1E') and US(x'1F').

APPEND

The transferred file will be appended to an existing PC file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing PC file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

DSTADDR(dstaddr)

This option specifies the destination address of the host to be used for the file transfer.

USERID(usr)

This option specifies the user ID to be used for the file transfer.

PASSWORD(pwd)

This option specifies the password to be used for the file transfer.

Send binary options (OS/400)



Options include:

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is removed from the end of each record. EOF (x'1A') is removed from the end of a file.

APPEND

The transferred file will be appended to an existing host file that has the same name (and type and mode for VM/CMS), if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

DSTADDR(dstaddr)

This option specifies the destination address of the host to be used for the file transfer.

USERID(usr)

This option specifies the user ID to be used for the file transfer.

PASSWORD(pwd)

This option specifies the password to be used for the file transfer.

SRC

This option specifies the OS/400 file type to be used for the transfer. If the host file does not exist, then a new file is created with the file type "Source physical file". This option is applicable only for the files in the QSYS library file system.

DTA

This option specifies the OS/400 file type to be used for the transfer. If the host file does not exist, then a new file is created with the file type "Physical data file". This option is applicable only for the files in the QSYS library file system.

SAVF

This option specifies the OS/400 file type to be used for the file send. If the host file does not exist, a new file is created with the file type "save file". If this option is specified, then the transfer mode must be binary. Also, this option is applicable only for files under the QSYS library file system.

LRECL(n)

This option specifies the logical record length when creating a file on the OS/400. It can have the following values:

- An integer from 1 through 32766 when **Host File Type** is set to **Source physical file**.
- An integer from 1 through 32754 when **Host File Type** is set to **Physical data file**.
- It is ignored when **Host File Type** is set to **Save file**.



Microsoft Internet Explorer users may see this error message in the java console while transferring files to the OS/400:

com.ms.SecurityExceptionEx[com/ibm/as400/access/SystemProperties/GetProperty]:
Unable to access system property: com.ibm.as400.Trace.category

This message can be ignored. If you want to remove the error message from the java console you can update the Windows registry entry

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM\classpath

with the Host On-Demand server directory, for example *c:\hostondemand\hod*.

Receive binary options (OS/400)



Options include:

CRLF

Carriage Return and Line Feed. CRLF (x'0D0A') is added at the end of each record. EOF (x'1A') is added at the end of the file. If APPEND is specified, EOF is removed from the end of an existing file and is added at the end of an appended file.

APPEND

The transferred file will be appended to an existing PC file that has the same name, if one exists. If APPEND is not specified, the transferred file overwrites the existing host file.

NEW

The transfer stops if the file already exists. This option can be used to protect against accidentally erasing an existing file.

DSTADDR(dstaddr)

This option specifies the destination address of the host to be used for the file transfer.

USERID(usr)

This option specifies the user ID to be used for the file transfer.

PASSWORD(pwd)

This option specifies the password to be used for the file transfer.

Connection tab



[Session Name](#)

[Destination Address](#)

[Destination Port](#)

[Anonymous Login](#)

[E-mail Address](#)

[User ID](#)

[Password](#)

[Account](#)

[Local Home Directory](#)

[Remote Home Directory](#)

[Load Initial Remote Directory](#)

[Lock](#)

Session Name

The name you want your session to have. The name appears beneath the session's icon and at the top of the session window.

Destination Address

The host name or TCP/IP address of the FTP server to which you want the session to connect. This can also be the Host On-Demand server (if the session will connect through the Redirector), a communications server/gateway or a host system.

Destination Port

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.

The default port is 21 for FTP.

Anonymous Login

Enables the session to login to an FTP server using *anonymous* as the user ID. If set to Yes and E-mail Address is blank the session also sends *anonymous* to the FTP server as the password.

The default is No

E-mail Address

Specifies the e-mail address to use when connecting to the FTP server while using Anonymous Login. If Anonymous Login is set to Yes, *anonymous* is used as the User ID, and the E-mail Address is used as the password. If E-mail Address is blank and Anonymous Login is set to Yes, *anonymous* is also used as the password.

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 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 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 on 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 on 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

Select Yes to view the initial host directory listing in the main FTP window. 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.

Lock (Host On-Demand Administrator only)

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Advanced tab

[If file exists](#)

[Confirm before Delete](#)

[Transfer Mode](#)

[ASCII File Types](#)

[Edit ASCII File Types](#)

[Start Automatically](#)

[Start in Separate Window](#)

[Auto-Connect](#)

[Auto-Reconnect](#)

[Timeout](#)

[Delay \(milliseconds\)](#)

[Number of Retries](#)

[Lock](#)

If file exists

Determines what action the session takes if the file already exists. 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 [Transfer List Manager](#) in the FTP client ignores this value.

The default is Prompt for Action.

Confirm before Delete

Prompts for confirmation before a file is deleted.

The default is Yes.

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 be executable, 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 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 clicking on them and click Remove. Click OK when you are finished editing ASCII File Types.

Start Automatically

Starts and connects the session (if Auto-Connect is Yes) when the client is loaded.

The default is No.

Start in Separate Window

If Yes is selected, 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.

The default is Yes.

Auto-Connect

Automatically connects the session to the target ftp 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

When set to Yes, automatically re-connects the session to the target ftp server if the connection fails. If you set this to No, you must click **Connect** in the session menu to re-connect the session.

The default is Yes.

Timeout (milliseconds)

Sets the FTP 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.

Lock (Host On-Demand Administrator only)

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

More Advanced tab



- [Data Connection Mode](#)
- [Startup Quote Command](#)
- [Host Type](#)
- [Encoding Type](#)
- [Language](#)
- [Transfer List Error](#)
- [Force BIDI reordering \(BIDI only\)](#)

Data Connection Mode

If you select Automatic, the FTP client attempts active mode transfer. If active mode transfer fails, the FTP client attempts passive (PASV) mode transfer. If PASV mode transfer works, the current session remains in PASV mode.

If you select Active, the FTP client always uses active/normal mode for data connection.

If you select Passive, the FTP client always uses passive mode for data connection.

The default is Automatic.

Notes:

- By default, the FTP client checks the socks settings in your browser's proxy server settings to automatically enable PASV mode. This option is ignored when your browser's proxy setting is enabled.
- When the FTP client is within a firewall and it detects that the FTP server is outside the firewall, passive (PASV) mode is automatically activated, if your browser's socks setting is enabled.
- If you have a socksified client, you must enable this option, if the FTP server is outside the firewall.
- If the FTP client is having trouble connecting to the FTP server, you may need to turn off the browser's proxy settings; if you have enabled this option, disable it.
- If the FTP client session appears to hang after a file upload or download when PASV mode is enabled, increasing the Timeout value on the [Advanced tab](#) from 60000 milliseconds to 120000 milliseconds might resolve the problem.

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.

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).

To list the contents of MVS datasets and HFS directories without changing the Host Type or defining two separate FTP sessions, select Auto-Detect for the Host Type. You can list the contents of either PDS datasets or HFS directories using the working Directory field. For example, the path user.linklib lists the members of the user.linklib dataset, and the path /usr lists the contents of the usr HFS directory.

When you select Auto-Detect, the FTP client uses SYST or PWD response string to determine the server directory style, and to parse the data in one of the Host Type formats. The following is the default Server OS and Host Type mapping based on SYST or PWD response:

Server OS Type	Host Type
----------------	-----------

OS/390 or z/OS	MVS or Unix
VMS or OpenVMS	OpenVMS
OS/2	OS/2
OS/400 v4r3 or lower (Library File System)	OS/400
OS/400 v4r4 or higher (IFS File System)	OS/400-Unix
Unix	Unix
VM	VM
Novell	Novell
Linux	Unix
Windows Systems	Unix or MS-DOS
Other Systems	Unix

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.

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.

Force BIDI reordering (BIDI only)

Enabled only if you select UTF-8 as the Encoding Type and Arabic or Hebrew as the Language. If file names in the FTP client appear in reverse, select Yes to reorder them. For more information, see [Bidirectional support for FTP client in UTF-8 mode](#).

Lock (Host On-Demand Administrator only)

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Screen tab



[Layout View](#)

[Toolbar](#)

[Toolbar Text](#)

[Status Bar](#)

[Transfer List Manager](#)

[Confirm on Exit](#)

[Lock](#)

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.

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 status bar displays all FTP commands and responses.

The default is Yes (visible).

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).

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.

The default is No.

Lock (Host On-Demand Administrator only)

Select Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Changing a file transfer list

You can update or delete lists when the Send or Receive windows are open.

To update a transfer list:

1. Click Open List and select the list you want to update; its contents appear in the Transfer List box.
2. If you want to change an entry in the list, select the entry; its parts are displayed in the Add File to Transfer List box.
3. Make the changes and click Update in List.
You can also [add files to the list](#).
To remove a file from the list, select it and click Remove.
4. Click Save List.

To delete a transfer list:

1. Click Delete List.
2. Select the list you want to delete.
3. Click OK.

FTP client session window



The FTP client session window displays two panels: a local file system panel and a remote file system panel. The working directory is displayed at the top of each panel. Actions only apply to the panel that currently has focus (the other panel appears greyed out). The buttons next to the working directory field allow you to move up one directory and create a new directory within the working directory. The buttons between the two panels allow you to transfer the selected files or directories into the destination's working directory.

- [View menu](#)
- [Actions menu](#)

View menu

The View menu gives you the following options:

Toolbar

Allows you to display or hide the Toolbar icons.

Toolbar Text

Allows you to display or hide the names of the Toolbar icons.

Status Bar

The status bar at the bottom of the session window displays all commands and responses from the FTP server for the session. You can configure the status bar on the session to be displayed or hidden.

Transfer List Manager

Allows you to display or hide the [Transfer List Manager](#) toolbar.

Side-by-side View

You can configure the panels to display the file systems side-by-side from within the session.

Stacked View

You can configure the panels to display the file systems stacked (one on top of the other) from within the session.

Refresh

Updates the FTP client window with your changes.

Host Directory Listing

A window appears displaying the server directory information for the directory you selected, including all attributes provided by the FTP server. If you select a different directory, the information for that directory appears at the end of the existing list. If you close the Host Directory Listing window and select Host Directory Listing again, only the information for the current directory appears.

Actions menu

The Actions menu gives you the following options:

Send files to/Receive files from Host

Sends selected files or directories to the FTP server from the local file system, or receives selected files or directories from the FTP server to the local file system. By holding down the Shift or Ctrl key, you can select multiple files or directories. You can also cancel file or directory transfers while they are in progress.

When If File Exists is set to Prompt For Action, you are presented with three choices:

- Overwrite, which replaces the file completely.

- Save As, which allows you to type a new name for the file.
- Skip, which allows you to choose not to transfer the current file.



When a file that is being uploaded is in different case than the one on the server, the client still generates an Overwrite Confirmation dialog. Some FTP servers allow storage of the same named file in different cases.

The FTP client's GUI component does not know the server platform so it cannot suppress the Overwrite Confirmation dialog. Just click the Overwrite button. The server version of the file will not be overwritten as long as the case is different.

Send files to Host as/Receive files from Host as

You can rename a file or directory before it is uploaded or downloaded to the receiving system. When renaming a directory, you cannot rename the files in the directory.

Send Transfer List to Host/Receive Transfer List from Host

Transfers the files in the current transfer list to/from the host. If you do not specify a directory for the local or remote file, then the FTP client attempts to find the file in the current working directory. If you send a list to the host and you do not specify a remote file name, the FTP client transfers the file with the local file name. If you receive a list from the host and you do not specify a local file name, the FTP client transfers the file with the remote file name. If a directory already exists, the FTP client overwrites only the files it transfers.

Note: The Transfer List Manager ignores the value for If File Exists in the FTP session properties on the [Advanced Tab](#). The Transfer List Manager always replaces an existing file.

Delete

Deletes the selected files or directories. You can select multiple files or directories to delete. If Confirm Before Delete is set to Yes, you are prompted to confirm the deletion. Also, if you select multiple files or directories, you will be prompted for confirmation for each file or directory before it is deleted. If you don't want to delete the current file or directory, click skip and you will be asked to confirm the deletion of the next file or directory.

Rename

Renames the selected file or directory. If you select more than one file or directory, you will be prompted for the new name for each file or directory. If you have selected multiple files or directories and do not want to rename the current file or directory, click skip, and you will be asked to rename the next file or directory.

Create Directory

Creates a sub-directory in the working directory. If the working directory is not where you would like to create a sub-directory, change to correct directory and type the name for the sub-directory. You do not need to type in the full path, only the sub-directory name.

Quote Command

Sends an uninterpreted string of data to the FTP server. The Quote Command allows you to set FTP server supported options. For example, to set the host translation table, type "site trans [translation table name]" in the dialog box.

Codepage Converter

Launches the [Codepage Converter](#) window, where you can convert different file types and change the codepages of files in either binary or ASCII mode.

Add to Current Transfer List

Adds the currently-selected files or directories to the current [transfer list](#) in the current transfer mode. The current working directory paths are added to each file. If you want to upload or download files to a different directory, you must manually add files to a transfer list.

Related topics

- [FTP client overview](#)

Transfer List Manager

The Transfer List Manager allows you to create file or directory transfer lists. Using the buttons on the Transfer List Manager toolbar, you can create a new list, delete a list, edit a list, edit list entries, and upload or download a list. List entries include a local file or directory name and path, a remote file or directory name and path, and the transfer mode for each file or directory.

List entries do not include a transfer direction. You can use a list to send or receive files or directories. If you select Send List to Host, the FTP client transfers files or directories in the Local column to the file or directory you select in the Remote column. If you select Receive List from Host, the FTP client transfers files or directories from the Remote column to the file or directory you select in the Local column.

During the file or directory transfer, if a source file does not exist, a message appears that allows you to continue to the next file in the list or cancel the transfer.

Note: The Transfer List Manager ignores the value for If File Exists in the FTP session properties on the [Advanced Tab](#). The Transfer List Manager always replaces an existing file.

Transfer List Manager toolbar

Send List to Host/Receive List from Host

Transfers the files in the current transfer list to/from the host. If you do not specify a directory for the local or remote file, then the FTP client attempts to find the file in the current working directory. If you send a list to the host and you do not specify a remote file name, the FTP client transfers the file with the local file name. If you receive a list from the host and you do not specify a local file name, the FTP client transfers the file with the remote file name. If a directory already exists, the FTP client overwrites only the files it transfers.

If you want the transfer to continue uninterrupted if a transfer error occurs, select Continue for [Transfer List Error](#) on the FTP session properties More Advanced Tab.

[Edit Transfer List](#)

Shows the current files in the transfer list.

Delete Transfer List

Deletes the currently selected transfer list.

Create New Transfer List

Allows you to create a new transfer list.

New Transfer List

Name

Type the name of the new transfer list.

Edit Transfer List

The Edit Transfer List window allows you to make changes to the current transfer list.

If you click Add, the Add File window appears, where you can add an entry to the transfer list.

Select one or more entries and click Update if you want to change the local file name, the remote file name, or the transfer mode.

Select one or more entries and click Remove to delete it from the list.

Click OK to save your changes.

Click Cancel to exit this window without saving your changes.

Add File

PC File Name

Type the name of the local file or directory. If you do not specify a path, the FTP client attempts to find the file in the current local directory.

Host File Name

Type the name of the remote file or directory. If you do not specify a path, the FTP client attempts to find the file in the current remote directory.

If you transfer a directory, do not follow the directory name with a forward or backward slash. For example, if you want to transfer directory Test6, type the following path name: D:\Test6

If you launch the FTP client from Windows or OS/2, use a backward slash to separate directory and file names.

If you launch the FTP client from UNIX, use a forward slash to separate directory and file names.

Transfer Mode

Select a [transfer mode](#).

OS/390 or z/OS MVS Services

If you add a file to a transfer list that exists on the MVS Services side of OS/390 or z/OS, the directory must be in single quotes followed by a forward slash. For example:

'MDBLAIR'/CLASS

Transfers *CLASS* from the MVS Service MDBLAIR

'TEST.SPF.ISPROF'/testfile

Transfers *testfile* from the MVS Service TEST.SPF.ISPROF

If you add a file to the transfer list that exists on the HFS side, add it as you would add a file on UNIX.

OS/400

On versions of OS/400 earlier than V4R4, add a file to a transfer list in the following format: LIBRARY/file.member

For example:

TEST/text.file1

Transfers the member *file1* from the file *text* in the library TEST.

On versions of OS/400 later than V4R4, add a file to a transfer list as you would on UNIX.

Codepage converter



You can use the Codepage converter to convert local files from one codepage to another. If you want to convert a remote file, you must download it first. The Codepage converter can convert more than one file at a time. The Codepage converter processes the changes for files downloaded in either ASCII or binary mode.

The Host On-Demand FTP client does not automatically convert files from one codepage to another. If you use the FTP client to transfer files and you want to convert codepages, you must use the Codepage Converter to convert files before upload and after download.

Starting the Codepage converter

From the FTP client, click Actions > Codepage converter.

Using the Codepage converter

- Select one of the following supported languages:
 - Arabic
 - Hebrew
 - Central Europe
 - Greek
 - Japanese
 - Korean
 - Latin
 - Russian
 - Thai
 - Turkish
 - Chinese Simplified
 - Chinese Traditional
- Select the transfer mode: ASCII or binary. If you select binary mode, select the host type for the input and output files.

If you want to use the binary mode for a mainframe codepage (z/OS or OS/400), set the record length for the file. The Codepage converter does not process files created with variable record lengths.

Input File

- Type the name of the input file in the Name field or click Browse to select a file. Select the current codepage of the Input File. The following table lists the supported codepages for each language.

Language	Codepage	Description
Arabic	8859_6	Arabic ISO code page for AIX
	Cp1256	Arabic PC code page for Windows 95 and Windows NT
	Cp864	Arabic PC code page for OS/2
	Cp420	EBCDIC Arabic
Hebrew	8859_8	Hebrew ISO code page for AIX
	Cp1255	Hebrew PC code page for Windows 95 and Windows NT

	Cp862	Hebrew PC code page for OS/2
	Cp856	Hebrew code page for AIX
	Cp424	EBCDIC Hebrew
	Cp803	EBCDIC Hebrew
Central Europe	8859_2	ISO 8859-2, Latin-2
	Cp1153	EBCDIC Latin-2 Multilingual, Euro support
	Cp852	PC Latin-2 codepage
	Cp870	EBCDIC Latin-2 Multilingual
Greek	8859_7	ISO 8859-7, Latin/Greek
	Cp869	Modern Greek PC codepage
	Cp875	EBCDIC Greek
Japanese	Cp1390	EBCDIC Mixed Byte Japanese Katakana-Kanji codepage
	Cp1399	EBCDIC Mixed Byte Japanese codepage
	Cp290	EBCDIC Single Byte Japanese Katakana codepage
	Cp930	EBCDIC Mixed Byte Japanese Katakana-Kanji codepage
	Cp939	EBCDIC Mixed Byte Japanese Latin-Kanji codepage
	Cp942	PC Japanese codepage
Korean	Cp1364	EBCDIC Mixed Byte Korean codepage
	Cp933	EBCDIC Mixed Byte Korean codepage
	Cp949	Korean PC codepage
Latin	8859_1	ISO 8859-1, Latin-1
	Cp037	EBCDIC USA, Canada, Australia, New Zealand, France, Portugal, Brazil
	Cp1046	Arabic codepage for Windows
	Cp1047	Latin-1, open systems
	Cp1140	EBCDIC US and others, Euro support
	Cp1141	EBCDIC Austria and Germany, Euro support
	Cp1142	EBCDIC Denmark and Norway, Euro support
	Cp1143	EBCDIC Finland and Sweden, Euro support
	Cp1144	EBCDIC Italy, Euro support
	Cp1145	EBCDIC Spain and Latin America, Euro support
	Cp1146	EBCDIC United Kingdom, Euro support
	Cp1147	EBCDIC France, Euro support
	Cp1148	EBCDIC Latin-1, Euro support
	Cp1149	EBCDIC Iceland, Euro support
	Cp273	EBCDIC Austria, Germany
	Cp274	Belgium (old)
	Cp275	Brazil
	Cp277	EBCDIC Denmark, Norway
	Cp278	EBCDIC Finland, Sweden
	Cp280	EBCDIC Italy
	Cp284	EBCDIC Spain, Latin America
	Cp285	IBM United Kingdom, Ireland
	Cp297	EBCDIC France
	Cp437	PC codepage for United States, Australia, New Zealand, and South Africa
	Cp500	EBCDIC Latin-1
	Cp850	PC Latin-1 codepage

	Cp871	EBCDIC Iceland
	Cp924	EBCDIC Latin-9
Russian	8859_5	ISO 8859-5, Latin/Cyrillic
	Cp1025	EBCDIC Cyrillic (Multilingual)
	Cp1112	EBCDIC Latvia, Lithuania
	Cp1122	EBCDIC Estonia
	Cp1123	EBCDIC Ukraine
	Cp1154	EBCDIC Cyrillic (Multilingual), Euro support
	Cp1156	EBCDIC Baltic (Multilingual), Euro support
	Cp1157	EBCDIC Estonia, Euro support
	Cp1158	EBCDIC Cyrillic and Ukraine, Euro support
	Cp855	Cyrillic PC codepage
	Cp866	Russian PC codepage
Thai	Cp1160	Thai with Low Tone Marks and Ancient Characters
	Cp838	EBCDIC Thai
	Cp874	Thai PC codepage
Turkish	8859_9	ISO 8859-9, Latin/Turkish
	Cp1026	EBCDIC Turkey
	Cp1155	EBCDIC Turkey, Euro support
	Cp857	Turkish PC codepage
Chinese Simplified	Cp1381	Simplified Chinese PC codepage
	Cp1388	EBCDIC Simplified Chinese
	Cp935	EBCDIC Mixed Byte, Simplified Chinese
Chinese Traditional	Cp1371	EBCDIC Traditional Chinese
	Cp937	EBCDIC Mixed Byte, Traditional Chinese
	Cp948	Traditional Chinese codepage for OS/2
	Cp950	Traditional Chinese PC codepage
	Cp964	Traditional Chinese codepage for AIX

Bidirectional support

If you select Arabic or Hebrew, you can choose the text type and text orientation of the input file.

- Select the current text type of the input file. The default is Logical.
- Select the current text orientation of the input file. The default is Left to Right.

Output File

- Type the name of the Output File or click Browse to select a file.
- Select the codepage for the Output File. The codepage for the Output File must be different from the codepage for the Input File.

Bidirectional support

If you select Arabic or Hebrew, you can choose the text type and text orientation of the output file.

- Select the Text Type for the Output File. The default is Logical.
- Select the text orientation of the output file. The default is Left to Right.

Symmetric Swapping

Symmetric swapping is only available for Arabic and Hebrew. If you want to force symmetric swapping, select Symmetric Swapping.

LamAlef Transform and Numeral Shape

The LamAlef Transform and Numeral Shape options are available only for Arabic. If LamAlef is enabled and if the Input File is Visual and the Output File is Logical, then the expansion function is applied to all LamAlef characters in the Input File (one lamalef character is expanded to two characters - lam followed by alef).

If the Input File is Logical and the Output File is Visual, then the compression function is applied to all LamAlef characters in the Input File (two characters lam and alef are compressed to one visual character).

If LamAlef is disabled, no expansion and compression can be done during the conversion.

Starting the conversion

Once you complete the previous steps, click Start Conversion to start the conversion.

Converting more than one file

If you want to convert more than one file, after you type the name of the output file, click Add to list. The input file and output file names appear in the Input File and Output File list, for example, infile1.txt outfile1.txt. The Codepage converter converts all files in the Input File and Output File list when you click Start Conversion.

Making changes to the selected files

1. Highlight the input file and output file to change the conversion configuration.
2. Click Edit.
3. Make changes to the input file and output file parameters.
4. Click Update in List to save your changes.
5. Click Start Conversion. All the files in the Input File and Output File list will be converted.

Removing a file from the Input File and Output File list

To remove a file from the Input File and Output File list, select the file you want to remove and click Remove.

Exiting the Codepage converter

To close the Codepage converter window, click Close.



Obtaining a server certificate



Certificates can be obtained from one of the following:

[Well-known Certificate Authority \(CA\)](#)

Create a certificate request, then obtain and store a server certificate from one of the pre-defined (well-known) CAs. This procedure requires the least setup because the Host On-Demand key database files already include the root certificates of several CAs.

[Unknown CA](#)

Create a certificate request, then obtain a server certificate and a root certificate from a CA that does not have its root certificate already included in the database. Having obtained the certificates, you must store them in the key database files.

[Self-signed](#)

You can create a certificate and use it while you are waiting for a CA's certificate, which can take some time. If you think the self-signed certificate provides adequate security, you can use it permanently.

Host On-Demand provides two ways to create certificate requests and self-signed certificates, and storing certificates in a key database:

- Certificate Wizard (Windows only)
- Certificate Management (Windows and AIX only)

Related topics

- [How SSL works](#)
- [Examples of when to use SSL](#)
- [Server authentication](#)



Making server certificates available



to clients

The following is a summary of the steps required to make a certificate available to download clients that connect securely to the Redirector or any other telnet server.

1. If the clients connect to a server, obtain a copy of the server's certificate. The Redirector's certificate can be extracted directly when created or received in Certificate Wizard and Certificate Management.
2. Add the certificate to the certificate container, CustomizedCAs.class.
3. Make CustomizedCAs.class available to clients.

To do this with the Certificate Wizard, start the wizard and select Import certificate. When you import a certificate, it is stored in the CustomizedCAs.class file.

To do this with the Certificate Management utility:

1. On a Windows server, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificateManagement from a command prompt. The default location of the AIX script is /usr/opt/hostondemand/bin. Please refer to [Running Certificate Management on AIX](#).
3. Follow the instructions in the Help for making certificates available to clients.
4. Exit Certificate Management.

When you have finished working with certificates, you must [configure the Host On-Demand clients](#) to use SSL.

Related topics

- [How SSL works](#)
- [Server authentication](#)



Using a server certificate from a



well-known (trusted) CA

The following root certificates are already stored in the key database and marked as trusted. Host On-Demand clients will trust certificates from these CAs:

- VeriSign Class 2 Public Primary CA
- VeriSign Class 2 Persona Not Validated
- VeriSign Class 3 Public Primary CA
- VeriSign Class 3 Persona Not Validated
- VeriSign Class 4 Public Primary CA
- RSA Secure Server CA (also obtained from VeriSign)
- Thawte Server CA
- Thawte Premium Server CA

To obtain and use a server certificate issued by a well-known (trusted) CA:

- [Create a certificate request](#).
- [Submit the request](#) to one of the CAs.
- When you receive the certificate, [store it in the server's key database](#).

Creating a certificate request

To create the certificate request:

Certificate Wizard:

1. Click Start > Programs > IBM Host On-Demand > Administration > Certificate Wizard.
2. Click Create a Certificate Request and follow the directions provided.

Certificate Management:

1. On Windows, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificatedManagement from a command prompt. The default location of the AIX script is /usr/opt/hostondemand/bin. Refer to [Running Certificate Management on AIX](#) for additional information.
3. Follow the steps in the Help to create the certificate request.
4. Exit Certificate Management.

Sending the certificate request to the CA

Go to the CA's Web site. Follow the instructions to submit the certificate request. Here are the URLs of the well-known CAs:

- VeriSign: <http://www.verisign.com/>
- Thawte: <http://www.thawte.com/>

While you are waiting for the CA to process your certificate request, you can enable security by [creating a self-signed root certificate](#).

Storing the certificate in the key database

When you receive the certificate, make sure it is in armored-64 or binary DER format. Only a certificate in one of these formats can be stored in the key database. The Certificate Wizard and Certificate Management programs can only accept simple certificates. They cannot accept certificate chains or PKCS7 data. The armored-64 form of a simple certificate starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----".

Store the certificate into the server's key database, HODServerKeyDb.kdb.

Certificate Wizard:

1. Start the Certificate Wizard, click Import a certificate, and follow the directions provided.
2. [Stop and restart the Service Manager](#).
3. [Make the certificates available to clients](#) (automatically done by the wizard).

Certificate Management:

1. On Windows, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificatedManagement from a command prompt. The default location of the AIX script is /usr/opt/hostondemand/bin. Refer to [Running Certificate Management on AIX](#) for additional information.
3. Follow the steps in the Help to store the certificate.
4. Exit Certificate Management.

Related topic:

- [How SSL works](#)
- [Server authentication](#)



Using a server certificate from an



unknown CA

An unknown CA is a CA that is not already defined in the key database or in the CustomizedCAs class files. To obtain and use a certificate issued by an unknown CA:

1. [Create a certificate request.](#)
2. [Submit the request to a CA.](#)
3. When you have received the server and root certificates from the CA, [store them in the key database](#). The root certificate may be sent to you with the server certificate but you can often get it from the CA's Web site.
4. [Make the certificate available to clients.](#)

After creating and submitting a certificate request to a CA, you can create a self-signed certificate to use while you wait to receive the CA's certificate.

Creating a certificate request

To create the certificate request:

Certificate Wizard:

1. Click Start > Programs > IBM Host On-Demand > Administration > Certificate Wizard.
2. Click Create a Certificate Request and follow the directions provided.

Certificate Management:

1. On Windows, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificateManagement from a command prompt. The default location of the AIX script is /usr/opt/hostondemand/bin. Please refer to [Running Certificate Management on AIX](#).
3. Follow the instructions in the Help to create the certificate request.
4. Exit Certificate Management.

When a certificate expires, follow the renewal procedures specified by the CA for that certificate.

Sending the certificate request to the CA

Start a browser and type the URL of the CA from whom you want to obtain the certificate, then follow the instructions to request the certificate.

Depending on the CA you choose, you can either e-mail the certificate request or incorporate it into the form or file provided by the CA. At the same time, ask for the CA's root certificate, though you can often get this directly from the Web site.

While you are waiting for the CA to process your certificate request, you can [create a self-signed root certificate](#) to use temporarily.

Storing the certificates in the key database

When you receive the certificates, make sure that they are in armored-64 or binary DER format. Only certificates in these formats can be stored in the key database. The Certificate Wizard and Certificate Management programs can only accept simple certificates. They cannot accept certificate chains or PKCS7 data. The armored-64 form of a simple certificate

starts with "----BEGIN CERTIFICATE----" and ends with "----END CERTIFICATE----".

Use the Certificate Wizard or Certificate Management to store certificates in the key database. You must store the root certificate *before* you store the server certificate because the root certificate is used to validate the server certificate.

Certificate Wizard:

1. Start the Certificate Wizard and select Import a certificate.
2. [Stop and restart the Service Manager.](#)
3. [Make the CA's root certificates available to clients.](#)

Certificate Management:

1. On Windows, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificatedManagement from a command prompt. The default location of the AIX script is /usr/opt/hostondemand/bin. Refer to [Running Certificate Management on AIX](#) for additional information.
3. Follow the steps in the Help to store the certificate.
4. Exit Certificate Management.

Related topic:

- [How SSL works](#)
- [Server authentication](#)



Using a self-signed certificate



If you decide not to purchase a CA's certificate, you can create your own (self-signed) server or client certificate. You can also use a self-signed certificate while you are waiting for a certificate from a CA, which can take some time.

Note:

You cannot use the Certificate Wizard to create a self-signed certificate on a locally-installed client.

To create and use a self-signed certificate:

Certificate Wizard:

1. Click Start > Programs > IBM Host On-Demand > Administration > Certificate Wizard.
2. Click Create Self-Signed Certificate and follow the directions provided.

If this is a client certificate, you will need to export it to a PKCS12 file.

Certificate Management:

1. On a Windows NT server, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificateManagement from a command prompt. The default location of the AIX script is `/usr/opt/server_dir/bin`. Refer to [Running Certificate Management on AIX](#) for additional information.
3. Follow the instructions in the Help to create the self-signed certificate.
4. If this is a server certificate, store it in the HODServerKeyDb.kdb database and then [make it available to clients](#). If this is a client certificate, store it in the HODClientKeyDb.kdb database, export it to a password-protected PKCS12 file and then send the file and its password to the user. Make sure the file is secure when sent to the user. If a non-secure protocol such as e-mail, http or ftp is used to send the file over the Internet, the certificate's security can be compromised.
5. Exit Certificate Management.

Related topic:

- [How SSL works](#)
- [Server authentication](#)

Running Certificate Management on AIX

Before running Certificate Management on AIX, you must be in the `/usr/opt/hostondemand/bin` directory, and the `JAVA_HOME` environment variable must be set to the full path to your Java installation. For example, if your Java system is installed in `/usr/J1.1.6`, run Certificate Management by doing the following:

```
$cd /usr/opt/hostondemand/bin
$export JAVA_HOME=/usr/J1.1.6
$CertificateManagement
```

Related topic:

- [How SSL works](#)
- [Examples of when to use SSL](#)

Host On-Demand Service Manager



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

When you log on as the administrator, you may see the following error message:

```
The Host On-Demand client is using a Configuration Servlet URL:
file:/servlet/HODConfig/hod and
is unable to contact the Host On-Demand Service Manager for one of the following
reasons:
```

1. The Configuration Servlet is not installed, is not operational, or is not configured with the correct hostname and port number of the Service Manager.
2. The client's ConfigServerURL parameter does not point to the Configuration Servlet or is missing the /hod extension from the end of the URL.
3. A network problem has prevented the connection.
4. The Service Manager is not started, or is not operational.

Please contact your system administrator.

This message indicates the service manager is not running.

- On Windows NT and Windows 2000, the service manager runs as a service. From the Start menu, open Control Panel > Services and start the service manager. Make sure that its Startup mode is Automatic so that it starts every time the operating system starts.
- On other platforms, the service manager runs as a Java application. Make sure this application starts every time the operating system starts.

Starting the service manager

In the Windows environment, the service manager starts automatically (through the Startup Folder in Windows 95 and Windows 98 and as an automatically started service in NT and 2000) after installation. It can also be started manually from the Start menu under Administration in the IBM Host On-Demand folder on Windows 95 and Windows 98, or from the Services control panel on Windows NT and 2000.

In other environments, you must manually start the service manager as a Java application. Sample command files for OS/2, NetWare, AIX, UNIX, and iSeries are provided in `\hostondemand\lib\samples\CommandFiles`. After customizing the file, run it to start the service manager.

Stopping and restarting the Service Manager

On a Windows NT or Windows 2000 server:

1. Click Start > Settings > Control Panel.
2. Open the Services folder.
3. Select the Host On-Demand Service Manager.
4. Click Stop.
5. When the service has stopped, click Start.

On a Windows 95 or Windows 98 client:

1. Press Ctrl+Alt+Del once to open the Close Program window.
2. Highlight the **Java** task and then click End Task.
3. Restart the Service Manager through Host On-Demand Administration in the Start menu.

On an OS/2 server:

Press Ctrl+C in the OS/2 window in which you started the Service Manager.

On a NetWare server:

From the console, enter `java -exit` to stop the java NLM.

On a UNIX server:

1. 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 /usr/local/hostondemand
```

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

2. Enter **kill -9 20130** at the command prompt.
3. When the Host On-Demand service manager has stopped, restart it in the usual way.

On an iSeries server:

You will need `*JOBCTL`, `*SPLCTL`, `*SERVICE` and `*ALLOBJ` authority to use this command.

1. Logon to the iSeries with a security officer user profile, such as `QSECOFR`.
2. Type `ENDHODSVM` at the command line.

Related topics

- [Configuring, starting, and stopping the Host On-Demand Service Manager on iSeries](#)

Using the Macro Editor



The Macro Editor allows you to modify an existing macro or create new macros. The Macro Manager records macros using XML scripting. Using the Macro Editor, you don't need to know XML scripting to edit a macro. The Macro Editor creates and modifies the script for you based on your input.

After recording a macro, not only can you make changes to host screen definitions but you can use the Macro Editor to further customize and fine-tune it. For example, you might decide that the descriptors used to identify a screen when the macro was recorded were too general for your environment (too many other screens fit the same descriptors). You can add new descriptors or modify the existing ones. When recording with the Macro Manager, the macro is recorded in a single, sequential format. Using the macro editor, you can expand the macro to add looping for repeating screens and conditional logic to handle multiple screen paths in a host application.

When you record and play a macro, it is not a fixed sequence of screens and actions. Rather, for each screen that is displayed, the macro program searches defined screens until it "recognizes" the screen. It identifies the screen based on the descriptors defined for each screen (by default, the Macro Manager uses the number of fields and input fields on the screen). Once a screen is identified, it performs the actions defined for that screen. It then repeats these steps for each new screen it recognizes.

When you edit macros that were recorded using Host On-Demand V3 in the Macro Manager or Macro Editor, it is converted to the XML format and cannot be converted back to the V3 format.

Using the Macro Manager



To display the Macro Manager, click Macro Manager on the tool bar.

[Recording a macro](#)

[Playing a macro](#)

[Changing a macro](#)

[Editing a macro](#)

[Deleting a macro](#)

[Adding a smart wait](#)

[Adding a prompt](#)

[Adding a data extraction](#)

[Macro Manager exercise](#)

A macro is a sequence of commands that performs 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.

Macros can be recorded and played in two ways:

- Using only the buttons on the toolbar or functions in the Actions menu.
- Using the Macro Manager. The Macro Manager gives you advanced macro editing capability.
 - A macro is saved with the icon that launched the session in your account-file (HOD.[your_id].user) on the server from which the session was loaded. Therefore, other users cannot run your macros.
 - 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 they are all downloaded when you start the session in which they were recorded.



Editing macro screen definitions



The Screens tab lists all the screens that are defined in this macro. Each screen definition contains general information, descriptors used to recognize the screen, and the actions to take when this screen is recognized.

To edit a macro screen:

1. Click Macro Manager on the toolbar.
2. Select the macro from the list.
3. Click Edit.
4. Click the Screens tab and select a screen to modify from the Screen Name list.

General

Provides general information about the screen.

Description

Lists the descriptors that are used to recognize a screen.

Actions

The actions that are performed when the screen is recognized.

To add a new screen to the macro, select <new screen> from the Screen Name list, then add descriptors and actions.

To delete a screen, select the screen and click Delete Screen.

Recording a macro



1. Click Actions > Record Macro.
2. Click New.
3. Type a name for your macro.
4. 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.
5. Select Express Logon Feature if you are recording a macro to use the [Express Logon](#) feature. To use this feature, the session must be an SSL session and using client authentication. The 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](#).
6. Click OK.
7. In the host session, perform the task you want to record. Every key you press is recorded as part of the macro. To press keys you don't 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, click Edit. 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.

Related topics

- [Adding a smart wait](#)
- [Adding a prompt](#)
- [Adding a data extraction](#)
- [Recording an Express Logon macro](#)

Playing a macro



From the session toolbar:

1. Click Actions > Play Macro.
2. Select the macro from the list.
3. Click OK.

From the Macro Manager:

1. Click Macro Manager on the toolbar.
2. Select a macro from the selection list on the left.
3. Click Play.

The list contains all previously recorded macros. To change the name of a macro or a description, [edit](#) the macro.

To stop playing the macro, click Stop. To pause the macro, click Pause. Click Pause again to continue.

Changing a macro

There are three ways to modify a macro that you have recorded:

1. Record the macro again.
2. Append to the macro.
3. [Edit the macro](#).

To re-record or append to the macro:

1. Click Actions > Record Macro, click Record on the Macro toolbar, or click Record on the session toolbar.
2. Click Existing.
 - To replace the macro with a new one, click Overwrite.
 - To continue recording from the end, click Append.
3. Select the macro you want to change.
4. Click OK.
 - If you chose Overwrite, click OK to confirm that you want to replace the macro and begin recording.
 - If you chose Append, press the keys you want to add.



You can add keystrokes only to the end of a macro. You must play the macro all the way through first. This ensures that the host application is at the correct point.

5. Click Stop when you have finished.

Deleting a macro

1. Click Macro Manager on the toolbar.
2. Select the macro from the selection list at the left.
3. Click Delete and then OK to confirm.

Adding a smart wait

A Smart Wait causes a macro to wait during playback until it recognizes a screen according to conditions that you set. If the macro recognizes the screen within the timeout period, it continues. If it does not, it stops.

To add a smart wait:

1. Click Macro Manager on the toolbar.
2. Click Record.
3. When you get to the point at which you want to add a wait, click Smart Wait.
4. Choose or type the conditions you want to use, and set the timeout interval.
5. Click OK.

A macro can recognize a screen according to any or all of these conditions:

Field Count

The total number of host fields.

Input-Field Count

The total number of input fields (fields that you can type in).



The Macro Manager automatically records the number of fields for you.

Wait for OIA to Become Uninhibited

If checked, the OIA must become uninhibited (no data communication and you are able to enter keystrokes) before the macro continues.

Use Cursor Position

Identifies the screen by the cursor position.

Keyword

Any word that will appear on the screen and that you want the macro to recognize. You should try to choose a word that is unique to that screen.

Timeout

A value in milliseconds (for example, 10000 is 10 seconds). Until all the conditions that you define have been satisfied, the macro will wait for the time specified. If the timeout expires before all the conditions have been met, the macro will stop playing back and display a message telling you the line on which it failed.

A value less than or equal to zero adds an indefinite wait.

If the macro consistently times out too soon, edit the code to increase the value (WaitForScreen).

- If the number of fields in your host application screen varies from time to time, you will sometimes not get a match for the Smart Wait. If this happens, re-record the macro without specifying either type of field count.
- The Macro function performs automatic screen-recognition by watching the cursor position on each screen. Do not add a Smart Wait for every screen unless you are sure that the cursor is a sufficient way of recognizing a screen.



Adding a prompt to a macro

You can insert a prompt in a macro so that during playback you can type information that varies or that you do not want displayed. When a prompt is reached during playback, a window opens asking for the information, which is then sent to the host application.

For example, if the task is to start a session, which requires a user id and password, you can insert a prompt for the user id and another for the password.

To insert a prompt:

1. Start recording using the Macro Manager.
2. When you get to the point at which input is required, click Prompt.
3. Enter the information required. The default value is optional.
4. Click OK. You are then asked to type the information required. You must type whatever entry is required to make the host application continue as usual. If you selected *Is it a password?* on the Add a Prompt window, this information is not displayed during playback so it is safe to type your password.
5. Click OK when you have finished.

Related topics

- [Recording a Macro](#)

Adding a data extraction

1. Start recording using the Macro Manager.
2. When you get to the point at which you want to extract data, click Extract.
3. Hold the left mouse button down and drag a rectangle around the data you want to extract.
4. Release the mouse button. The Add an Extraction window appears.
5. Type a name. If you want to change the area you marked, adjust the coordinates or click Cancel and drag a new rectangle.
6. Click OK.

Name

Enter a name for the extraction.

Row and Column (top and bottom corners)

These are the coordinates for the area you marked.

Data Plane

Select one or more of the following planes to extract. You must select at least one plane.

TEXT_PLANE

The text plane contains the text on the screen.

COLOR_PLANE

The color plane contains color information for each character of the presentation space.

FIELD_PLANE

The field plane represents the field positions and their attributes in the presentation space.

EXFIELD_PLANE

The extended field plane contains extended character attribute data.

DBCS_PLANE

The DBCS plane contains double-byte character set attribute data for each character and field attribute in the presentation space. You can only select DBCS_PLANE when you are running a DBCS session.

GRID_PLANE

The grid plane contains information for displaying the grid.

A data extraction is intended for host-system application developers and administrators who want to create macros that retrieve data from a host application and put it into an applet or a graphical user interface by using the `MacroExtractEvent` method of the Host Access Class Library. Such macros might be distributed to application developers, who can use them to get data from a host application without knowing how the application is structured. This function has no significance in regards to playback through a Host On-Demand emulator.

See the Macro Script Syntax section of *Host Access Beans for Java* for macro coding information.

Macro Manager exercise



This exercise takes you through the recording features of the Macro Manager. Because host applications are so different, the steps will not apply to all host applications. It's up to you to customize the macro for your specific application.

In this exercise, IBM's OfficeVision/VM application is used. If your host uses OfficeVision, great! If not, comments in *italics* guide you in customizing a macro for your own application. A menu application will work best for this exercise (ISPF is a good one if you're using it with TSO). Before you start, be sure that a session is started and that you are logged on to your host system.

Don't forget to click the Help button if you need to!

1. Click Macro Manager on the toolbar.
2. Click Record.
3. Click New.
4. Enter the following information:
 - Name - Exer1
 - Description - Macro Recording Exercise (don't worry if the text wraps; it is stored as a continuous string)
5. Click OK. You are now in record mode. All keystrokes will be recorded in the macro.
6. At your host's system prompt, type **profs** and press Enter. *Substitute your application's command here. For example, if you use ISPF, from a TSO prompt type ispf instead of profs.*
7. Insert a Smart Wait. Click the Smart Wait button and do the following:
 - Check Field Count
 - Check Input Field Count
 - Enter OfficeVision/VM in the Keyword field (note: a Wait is case sensitive). *Substitute a keyword that is unique to the first screen of the host application.*
 - Enter 5000 in the Timeout field (5 second wait)



If the host application screen has a variable number of fields, you may not get a match for the smart wait because the number of fields recorded can be different from what is actually on the screen. If so, re-record the macro and don't use field counts.

8. Add a prompt for the menu item. Click Prompt and do the following:
 - Don't edit the row and column position. The cursor is already where it needs to be to enter OfficeVision commands. *If you need to adjust the location of where the prompt will be placed for your application, either adjust the values in the window, or click Cancel, move your cursor to the right place with your mouse (not with the arrow keys) and click the Prompt button again. If you are not using OfficeVision for this exercise, your cursor should be at the location where you enter menu commands.*
 - Name the prompt Enter Menu Choice.
 - Enter filelist as the default value. *Add a default menu command.*
9. Click OK. A prompt window appears. This allows you to enter whatever text the application needs in order to continue normally. Usually, you can leave the default value in the prompt window and click OK. The prompt places the text on the screen only; it doesn't press Enter because you might want to do something else, like press a PF key.
10. Press Enter. The filelist command is entered. *Press the key that will send the command to the host.*
11. Press PF11. This should bring you into XEDIT mode for the first file in the list.
12. Click Stop. You're done! *Do any steps you want recorded in the macro and then click Stop.*

Test the macro by going back to the screen from which you started, and click Play.



The Macro function performs automatic screen-recognition for you by watching the field counts on each screen. You don't have to add a smart wait for every screen unless you are sure that the field counts are not a positive enough way of recognizing a screen. IBM's Callup application is a good example of when you do need a smart wait, because the cursor position depends on how long a name you're searching for.

Related topics

- [MacroManager Overview](#)

Provides general information about the screen.

For any field except Screen Name, you can use a variable name or an arithmetic expression as the field value. You can enter these variable names and expressions directly into text areas or add them to lists by selecting <Expression> from the list.

A variable name should have the following format: `var_name`, where *var_name* can be alphanumeric, the dash symbol, and the underscore symbol. Variable names must be enclosed in dollar signs. Variable names are case sensitive.

Screen Name

Unique text string to identify the selected screen. Each screen within a macro must have a unique name. This is the name that appears in the Screen Name selection list.

Entry Screen

Select true if the selected screen is the first screen in the macro to be displayed. Only one screen can be identified as the entry screen.

Exit Screen

Select true if the selected screen is the last screen in the macro to be displayed. The macro stops playing when it comes to an exit screen.

Transient Screen

Select true if the selected screen is an intermittently displayed screen that appears at different times but always needs the same action applied. For example, you might have a screen that appears at different times in the macro, and simply needs to be cleared. Rather than identifying this screen as a Valid Next Screen for all screens that it might follow, you can mark it as a transient screen. When a transient screen is encountered, the defined actions are taken even though this screen is not on the previous screen's next screen list. The macro continues recognition of the next screen, essentially ignoring the transient screen. A transient screen can be matched at any point in the macro. Any Valid Next Screens for a transient screen are ignored.

Set Recognition Limit

Limits the number of times the current screen can be recognized by the macro. This field prevents infinite looping in the macro. If the Screens Before Error limit is reached, the macro will stop with an error.

Set Pause Time

Time to wait between actions associated with this screen after the screen has been displayed. If this option is not checked, the global [pause time value for the macro](#) will be used.

Related topics

- [Using the Macro Editor \(an overview\)](#)
- [Editing the XML script](#)
- [Importing a macro](#)
- [Exporting a macro](#)
- [Variables](#)

Description



Lists the descriptors that are used by the macro to identify a screen. More information about the macro script syntax can be found in the Host Access Beans for Java document included in the Host On-Demand Toolkit.

For any field except Screen Name, you can use a variable name or an arithmetic expression as the field value. You can enter these variable names and expressions directly into text areas or add them to lists by selecting a new descriptor or <Expression> from the list.

A variable name should have the following format: `var_name`, where *var_name* can be alphanumeric, the dash symbol, and the underscore symbol. Variable names must be enclosed in dollar signs. Variable names are case sensitive.

Descriptor

Lists all the descriptors defined for the selected screen. A descriptor is an attribute used by the macro to identify a screen. For each new screen that appears, the macro compares what is on the session window to the list of descriptors for each defined screen until a match is made. Descriptors should be as unique as possible to avoid multiple screens from matching one description. If this screen collision occurs, the wrong actions could be executed on the wrong screen. This could cause screen recognition failure at some point in the execution, resulting in a macro timeout error.

By default, when the Macro Manager records a macro, the OIA and field counts descriptors are defined to identify the screen. If this is adequate, you don't need to make any changes on this tab. However, we recommend that you add String descriptors for more strict and accurate screen recognition.

To modify a descriptor, select the descriptor from the Descriptor list. The name of each descriptor is created automatically based on the descriptor type and the contents of the descriptor. To create a new descriptor, choose the appropriate type of descriptor that you want to create (for example, <new string descriptor>). You can only have one Cursor and one Field Counts and OIA descriptor per screen. You can have multiple String and Attribute descriptors.

A screen is recognized by any of the following types of descriptors:

- [String](#)
Identifies the screen by text that appears on the screen
- [Cursor](#)
Identifies the screen by the cursor position
- [Attribute](#)
Identifies the screen by plane attributes (for example, color)
- [Field Counts and OIA](#)
Identifies the screen by number of fields, number of input fields, and OIA state
- [Variable Update](#)
Updates a variable with a new value

If you define more than one descriptor as optional, once the first optional descriptor is matched, the other optional descriptors are ignored.

To delete a defined descriptor, select it and click Delete.

Auto-Capture automatically creates descriptors based on the current values shown on the current session window. You can choose which descriptor types to define. Be sure that the correct session screen is showing when you use this option.

String

Identifies the screen based on a string displayed on the screen at a known position. Enter the row and column values or click the session screen and it is brought to the foreground. If the Macro Editor is open, you must move it for the session screen to be brought to the foreground. Select the string by drawing a rectangle around it. The start and end row and column fields will then be automatically filled in for you. Copy and paste the string in your selected area into the String field.

Start Row

Starting row position where the macro will look for the string starting from the top of the screen. A negative number starts the count from the bottom of the screen.

Start Column

Starting column position where the macro will look for the string, starting from the left-most column. Using a negative number starts the count from the right side of the screen.

End Row

Ending row position where the macro will look for the string in a rectangle. If both end row and end column are specified then the macro will look for the string in a rectangle.

End Column

Ending column position where the macro will look for the string in a rectangle. If both end row and end column are specified, then the macro will look for the string in a rectangle.

String

The string that is used to identify the screen.

Ignore Case

String is case sensitive if you select false.

Optional

The string is not required to recognize the screen. At least one optional descriptor must match for the screen to be recognized. Use this option, for example, if one of two strings might appear on the screen. You can define both as optional descriptors. At least one optional descriptor has to match for this screen to be identified, however. This option assumes you have more than one descriptor specified as optional. If only one descriptor is specified as optional, then it will be required.


Inverse Descriptor

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.



You can enter negative numbers for rows and columns. Negative numbers are virtual positions from the bottom row. If End Row and End Column are not specified, then Start Row and Start Column are used as absolute position.

Cursor

Identifies the screen based on the position of the cursor. Specify the cursor position, or click the position on the screen and click  to use the cursor's current position on the session screen if you know it's correct.

Row

Row position of the cursor.

Column

Column position of the cursor.

Optional

The cursor position is not required to recognize the screen. At least one optional descriptor must match for the screen to be recognized. Use this option, for example, if one of two cursor positions might appear on the screen.

You can define both as optional descriptors. At least one optional descriptor has to match for this screen to be identified. This option assumes you have more than one descriptor specified as optional. If only one descriptor is specified as optional, then it will be required.

Inverse Descriptor

If you select true, the cursor defined by this descriptor must not be at the specified cursor Row and Column.

Attributes

Identifies the screen by plane attributes (color, field, or extended field) at a specified row and column position. Specify the attribute position or click Current to use the cursor's current position on the session screen if you know it's correct.

Row

Row position of the attribute.

Column

Column position of the attribute.

Data Plane

Specifies the plane associated with the Attribute Value.

- FIELD_PLANE - represents the field positions and their attributes as they appear on the screen.
- COLOR_PLANE - contains color information for each character on the screen.
- EXFIELD_PLANE - extended character attribute data, for example, reverse image, underline, blink, double-byte characters, or character color.

Attribute Value

Hexadecimal value defining the attribute for this data plane. Click Edit Attributes to graphically choose the value.

Note: You do not need to enclose the Attribute Value in single quotes. For more information, see [Use Variables and Arithmetic Expressions in Macro](#).

Optional

The plane attribute is not required to recognize the screen. At least one optional descriptor must match for the screen to be recognized. Use this option, for example, if more than one attribute might appear on the screen. You can define both as optional descriptors. At least one optional descriptor has to match for this screen to be identified. This option assumes you have more than one descriptor specified as optional. If only one descriptor is specified as optional, then it will be required.

Inverse Descriptor

If you select true, the attribute defined by this descriptor must not appear on the session screen.

Field Counts and OIA

Identifies the screen by any of the following:

Number of Fields

The total number of fields on the screen.

Number of Input Fields

The total number of fields on the screen that are input fields.

Inverse Descriptor

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.

Wait for OIA to become Uninhibited

If you select true, and Optional is also true, the OIA is inhibited. If you select false and Optional is true, the OIA is

uninhibited (able to enter keystrokes).

Optional

Each of the above fields can be marked as optional and is not required to recognize the screen. Use this option, for example, if one of two field options might appear on the screen. You can define both as optional descriptors. At least one optional descriptor has to match for this screen to be identified. This option assumes you have more than one descriptor specified as optional. If only one descriptor is specified as optional, then it will be required.

Variable update

Updates a variable with a new value.

Name

Select the name of the variable to update.

Type

Displays the type of the currently selected variable. If the variable is not defined in the current macro, no type appears.

Value

Any valid expression, for example, 'hello', 5, or $\$var\$ + 1$.

Current Cursor Position

Click Current to assign the content of the screen at the current cursor position to a variable. When the macro runs, the content of the screen at the cursor position you specify becomes the value for the variable. Current is enabled only for field variables.

Actions

Lists the actions to be performed when a screen within a macro is recognized.

The Actions tab provides all of the actions to perform on the selected screen when it is identified by the macro. To modify an action, choose the action from the Action list. The name of each action is created automatically based on the action type and the contents of the action. To create a new action, choose the appropriate type of action you want to create (for example, <new input action>).

For any field except Screen Name, you can use a variable name or an arithmetic expression as the field value. You can enter these variable names and expressions directly into text areas or add them to lists by selecting <Expression> from the list. If you select <Expression> from the list and the only other options in the list are True and False, the expression must return either True or False.

A variable name should have the following format: `var_name`, where `var_name` can be alphanumeric, the dash symbol, and the underscore symbol. Variable names must be enclosed in dollar signs. Variable names are case sensitive.

If an action requires row and column values, you can click on the session window at the desired position and the values appear in the row and column field. Click once to give the session window focus, and again for the values of the position you select to appear in the row and column field.

- [Input](#)
Sends keystrokes to the screen.
- [Extract](#)
Extracts data from the screen.
- [Prompt](#)
Prompts the user for information while the macro is running.
- [Message](#)
Displays a message to the user.
- [Pause](#)
Pauses the macro for the specified amount of time.
- [Transfer](#)
Transfers a file to or from the host.
- [Comm wait](#)
Waits for a communication status.
- [Trace](#)
Writes out a trace record.
- [Mouse click](#)
Simulates a user mouse click.
- [Box select](#)
Marks an area on the screen.
- [Run program](#)
Runs a program while the macro plays.
- [Variable update](#)
Updates a variable with a new value.
- [Play macro](#)
Stops the currently running macro and starts playing the macro you specify.
- [Conditional](#)
Allows you to place conditions around actions.

To delete a defined action, select it and click Delete.

Click Order to change the order the actions should be performed on the screen.

More information about the macro script syntax can be found in the Host Access Beans for Java document included in the Host On-Demand Toolkit.

Input

Inputs a string or an action key, or both, at the selected position.

Row and column

Row and column define the position on the session screen to place the string.

String

String (including the action keys) that is placed on the session screen.

Action Keys

To enter an action key into the String field, select an action key and click Insert Action Key. The Action key appears at the end of String field.

Translate Host Action Keys

Translates host key mnemonics, for example [enter], as input for a field on the session screen.

Move Cursor to End of Input

Places the cursor at the end of the input string on the session screen.

Note: If action keys such as [tab], [up], or [down] are included in the String field, the Move Cursor to End of Input option is ignored by the macro. That is because the action keys require the cursor to move to a specific place on the screen.

Extract

A data extraction is intended for host-system application developers and administrators who want to create macros that retrieve data from a host application and put it into an applet or a graphical user interface by using the MacroExtractEvent class defined in the Host Access beans package. Such macros might be distributed to application developers, who can use them to get data from a host application without knowing how the application is structured.

Click the screen to select the area to be extracted from the session screen. Hold the left mouse button down and drag a rectangle around the data you want to extract.

Start Row and Start Column

Top left position of the bounding extract rectangle.

End Row and End Column

Bottom right position of the bounding extract rectangle.

Extraction Name

Name of the extraction. Use a name to identify what is being extracted from the session screen. This name is passed to the MacroExtractEvent.

Data Plane

Select one or more of the following planes to extract. You must select at least one plane.

TEXT_PLANE

The text plane contains the text on the screen. When you add a new extract action, TEXT_PLANE is the default data plane.

COLOR_PLANE

The color plane contains color information for each character of the presentation space.

FIELD_PLANE

The field plane represents the field positions and their attributes in the presentation space.

EXFIELD_PLANE

The extended field plane contains extended character attribute data.

DBCS_PLANE

The DBCS plane contains double-byte character set attribute data for each character and field attribute in the presentation space. You can only select DBCS_PLANE when you are running a DBCS session.

GRID_PLANE

The grid plane contains information for displaying the grid.

Unwrap Text

Unwrap text in a field that spans multiple lines on the screen.

Assign Text Plane to a Variable

Assigns the extracted texts into a specified variable.



You can enter negative numbers for rows and columns. Negative numbers are virtual positions from the bottom row.

Prompt

Prompts the user for information while the macro is running.

Row and Column

Identifies the row and column on the session screen where the macro will place the prompt response value. For example, if you prompt the user for a User ID, the value they enter will be placed on the screen in this location.

Prompt Name

Caption that appears in the title bar of the prompt message box.

Prompt Text

Text inside the prompt message box that asks the user for input. For example, if you are asking for a user ID, the prompt text can be: Enter your user ID.

Clear Host Field

Clears the host field before placing the prompt text. This is useful when host applications populate a host field when the screen is sent.

Default Response

Default value, if any, for the prompted response value. When the user is prompted, this value will be in the response field by default. The user can change this value.

Password Response

Hides the response for the prompt by displaying asterisks instead of the characters typed.

Response Length

The maximum length for the response value (number of characters).

Translate Host Action Keys

Accepts host key mnemonics, for example [enter], as input for a field on the session screen. The default is true.

Move Cursor to End of Input

Places the cursor at the end of the input value on the session screen for subsequent input actions. If action keys such as [tab], [up], or [down] are included in the String field, the Move Cursor to End of Input option is ignored by the macro. That is because the action keys require the cursor to move to a specific place on the screen.

Assign to a Variable

Assigns a user's input to a specified variable. If the variable is an integer, a double, a boolean, or a field, the user input or response must match, otherwise an error or unexpected result occurs. For more information about variable types, see the online help for [Variables](#).

Don't Write to Screen

Enabled only if you select Assign to a Variable. If you select true, the user's input is assigned to a variable, but does not appear on the screen. The default is false.



The prompt value is placed on the screen in the specified location. The enter key will not automatically be pressed. If you want the value entered, create a new Input action for the Enter action key.

Message

Displays a message to the user.

Message Title

Caption that appears in the title bar of the message window. The default is to use the macro name.

Message Text

Message displayed in the message window.

Pause

Pauses the macro for the specified amount of time.

Duration

Time in milliseconds to pause the macro when it is running.

Transfer

Transfers a file to or from a host. Click Advanced for more options.

Send/Receive

Select if you are sending or receiving files from the host.

Host File Name

Enter the name of the file that you are sending or receiving. The file name must be in the host file format.

PC File Name

Enter the path name and file you are sending or receiving. The file name must be in PC file format. Click Browse to locate the file on your system.

Advanced Options

Clear before Transfer

Clears the host screen before transferring the file. You should not change this setting because in nearly every case, CMS and CICS require that this command be sent, whereas TSO and OS/400 do not.

Timeout

Specify the length of time (in milliseconds) to wait for a file to transfer. If the transfer does not complete in this time, the macro ends and displays a message. The default is 10000 milliseconds, or 10 seconds.

Options

Enter the host specific options for the file transfer. Options are different for each type of host system.

PC Code-page

Select the PC code-page for the transfer. This code page should match the code-page set in the session configuration properties. The code-page is a table that translates EBCDIC codes to PC 1-byte codes, or vice versa, when files are transferred. Only valid code pages for your computer's locale are included in this list.

Host File Orientation

Specify whether the host files will be saved in left-to-right or right-to-left format. Use this option if the session is configured to use an Arabic or Hebrew host code-page. The default is left-to-right.

PC-File Orientation

Specify whether the PC files will be saved in left-to-right or right-to-left format. Use this option if the session is configured to use an Arabic or Hebrew host code-page. The default is left-to-right.

PC-File Type

Specify whether the PC files you transfer will be saved in the format in which they are saved (implicit) or in the format which they should be displayed. The default is implicit. Use this option if the session is configured to use an Arabic or Hebrew host code-page.

Lam-Alef Expansion

Specify if files containing the character *Lam_alef* should be expanded into two characters, *Lam* followed by *Alef*, when received from the host. Use this option if the session is configured to use an Arabic host code-page.

Lam-Alef Compression

Specify if files containing the characters *Lam* followed by *Alef* should be compressed into one character, *Lam_alef*, when sent to the host. Use this option if the session is configured to use an Arabic host code-page.

Symmetric Swapping

Specify whether brackets are reversed from the source to the target. If symmetric swapping is enabled, brackets are reversed from the source to the target. For example, (is replaced by) and) is replaced by (when host file orientation is right-to-left. If symmetric swapping is not enabled, the brackets are not reversed. Use this option if the session is configured for an Arabic or Hebrew host code-page and affects the brackets during file transfer.

Numerals Shape

Specify how numerals appear when sending files to the host. The Numerals Shape indicates one of the following:

- Nominal: all numerals are Arabic numerals
- National: all numerals are Hindi numerals
- Contextual: numerals appear Arabic after English text, or numerals appear Hindi after Arabic text

Use this option if the session is configured for an Arabic host code-page.

Round Trip

Specify that if numerals are preceded by Arabic characters, the numerals exchange places with the Arabic characters when transferring files. Use this option if the session is configured for an Arabic host code page.

Comm wait

Waits for a communication status from the host while the macro is running.

Connection Status

The type of communication status, as defined by the ECLConnection class, to wait for.

Timeout

Time to wait, in milliseconds, for the communication wait. If a status is not received by the specified time, that macro stops.

More information about the ECL Connection class can be found in the *Host Access Class Library for Java* document included with the Host On-Demand Toolkit.

Trace

Writes out a trace record.

Trace Handler

Where the trace text is sent.

- Host On-Demand Trace Facility
- User trace event to Java applet or application. This facility is intended for host-system application developers and administrators who want to track macro play using the MacroTraceEvent class defined in the Host Access beans package.
- Command line traces appear on the Java console of the Web browser that launched the Host On-Demand emulator.

Trace Text

Text sent to the trace handler.

Mouse click

Sets the cursor using a mouse click at the specified row and column.

Row and column

The host screen row and column position for the mouse click.

Box select

Marks an area on the screen, replacing a previous selection.

Row (top) and Column (top)

Top left row of the marked rectangle. These values must be numbers within the host screen coordinate system, for example, 24 rows by 80 columns. Negative numbers are virtual positions from the last row.

Row (bottom) and Column (bottom)

Bottom right row of the marked rectangle. These values must be numbers within the host screen coordinate system, for example, 24 rows by 80 columns. Negative numbers are virtual positions from the last row.

Run program

Runs a program while the macro plays.

Program

The name of the program.

Parameters

The program parameters.

Wait for Program

If you select true, the macro pauses until the program completes. The default is false.

Assign Exit Code to Variable

Enabled only if Wait for Program is true. Select a variable from the list.

Variable update

Updates a variable with a new value.

Name

Select the name of the variable to update.

Type

Displays the type of the currently selected macro. If the variable is not defined in the current macro, no type appears.

Value

Any valid expression, for example, 'hello', 5, or $\$var\$ + 1$.

Current

Click Current to assign the content of the screen at the current cursor position to a variable. When the macro runs, the content of the screen at the cursor position you specify becomes the value for the variable. Current is enabled only for field variables.

Play macro

Stops the currently running macro and starts playing the macro you specify. You can only select macros that are available in your current session.

Macro Name

Lists the available macros by name.

Macro Description

The description you gave the macro when you created it.

Start Screen Name

Lists all screens for the macro you select, as well as *DEFAULT*. If you select a specific screen from the list, the chained macro starts at the screen you specify. If you select *DEFAULT*, the macro starts at the screen you defined as the start screen when you created the macro.

Variable Transfer

If you select Transfer, all of the current variables are transferred to the next running macro. The default is No Transfer.

Conditional

Allows you to place conditions around actions. If you want to use the Conditional action, select Use Variables and Arithmetic Expressions in Macro on the [Macro tab](#) in the Macro Editor. Otherwise, your macro might not work as expected.

Condition

Type a valid condition, for example, $(\$varA\$ == 'abc') \&\& (\$varB\$!= 1)$. If you do not type a conditional, the default is true. The following table shows the syntax for conditionals:

Symbol	Definition
==	equal to
!=	not equal to
<	less than
>	greater than
<=	less than or equal to
>=	greater than or equal to
	or
&&	and
!	not

In this context, you can use parentheses to nest conditions. If you want to use an arithmetic expression with nested expressions (an expression containing parentheses) in your condition, you must first assign that expression to a variable and then use the variable in your condition. For example, you could create the following condition: $\$expression\$ == 21$ where $\$expression\$$ is a variable with the value $(5 + 2) * 3$.

Condition is true

The actions that appear in the Actions list will be performed on the screen if the condition is true. For each conditional action you create, you can specify one condition, along with a set of actions to perform if the condition is true and a different set of actions to perform if the condition is false.

Action

You can create any action for a conditional action except another conditional action.

- [Input](#)
Sends keystrokes to the screen.
- [Extract](#)
Extracts data from the screen.
- [Prompt](#)
Prompts the user for information while the macro is running.
- [Message](#)
Displays a message to the user.
- [Pause](#)
Pauses the macro for the specified amount of time.
- [Transfer](#)
Transfers a file to or from the host.
- [Comm wait](#)
Waits for a communication status.
- [Trace](#)
Writes out a trace record.
- [Mouse click](#)
Simulates a user mouse click.
- [Box select](#)
Marks an area on the screen.
- [Run program](#)
Runs any program that can be executed by the run time.
- [Variable update](#)
Updates a variable with a new value.
- [Play macro](#)
Stops the currently running macro and starts playing the macro you specify.

To delete a defined action, select it and click Delete.

Click Order to change the order the actions should be performed on the screen.

Condition is false

The actions that appear in the Actions list will be performed on the screen if the condition is false.

The Condition field is grayed out. For each conditional action you create, you can specify one condition, along with a set of actions to perform if the condition is true and a different set of actions to perform if the condition is false.

Action

You can create any action for a conditional action except another conditional action.

- [Input](#)
Sends keystrokes to the screen.
- [Extract](#)
Extracts data from the screen.
- [Prompt](#)
Prompts the user for information while the macro is running.
- [Message](#)
Displays a message to the user.
- [Pause](#)
Pauses the macro for the specified amount of time.
- [Transfer](#)
Transfers a file to or from the host.
- [Comm wait](#)
Waits for a communication status.
- [Trace](#)
Writes out a trace record.
- [Mouse click](#)

Simulates a user mouse click.

- [Box select](#)
Marks an area on the screen.
- [Run program](#)
Runs any program that can be executed by the run time.
- [Variable update](#)
Updates a variable with a new value.
- [Play macro](#)
Stops the currently running macro and starts playing the macro you specify.

To delete a defined action, select it and click Delete.

Click Order to change the order the actions should be performed on the screen.

Example of a conditional

In this example, your macro has a run program action that assigns an exit code to the variable \$exit\$ (0 if the program executes successfully, non-zero if not). You can use the conditional action to display one message if the exit code is 0 (success), and another message if the exit code is not zero (failure). Complete the following steps to create the conditional action:

1. In the Macro Editor, open your macro that runs the program.
2. On the Screens tab, select the screen with the run program action. On the Actions tab, select <new conditional action> from the Action list.
3. In the Condition field, type the condition \$exit\$ == 0.
4. On the Condition is True tab, select <new message action> from the Action list.
5. In the Message Text field, type 'Program executed successfully.'

If the condition is true, for example, the exit code for your program is 0, a message appears saying the program executed successfully. You can specify more actions on this tab. The macro performs these actions if the exit code is 0.

6. On the Condition is False tab, select <new message action> from the Action list.

Note: The Condition field is grayed out. For each conditional action you create, you can specify one condition, along with a set of actions to perform if the condition is true and a different set of actions to perform if the condition is false. Currently, there should be no actions defined on the Condition is False tab.

7. In the Message Text field, type 'Program exited abnormally with an exit code of: ' + \$exit\$

If the condition is false, for example, the exit code for your program is not 0, a message appears saying the program exited with an error and the exit code will be displayed. You can specify more actions on this tab. The macro performs these actions only if the exit code is not 0.

Your macro is now ready. If you select Edit Code on the Macro Editor window, you should see the following code:

```
<actions>
...
  <if condition="$exit$ == 0" >
    <message title="" value="'Program executed successfully' " />
  </if>
  <else>
    <message title="" value="'Program exited abnormally with an exit
code of: '+$exit$" />
  </else>
...
</actions>
```

Note: Toggling back and forth between the Condition is True tab and the Condition is False tab populates the Action list with the actions from the <if> block and the actions from the <else> block, respectively.

Related topics

- [Bidirectional language support](#)
- [Transferring files](#)
- [Variables](#)

Adding a Prompt

A prompt is a window that opens to request information from the user during macro playback.

Row and Column

The position in which the information is to be placed during playback. The values displayed show the current location of the cursor but you can change them.

Prompt Name

Enter the text that must appear next to the input box in the prompt window during playback. For example, if you are inserting a prompt for a user id, the prompt text could be User ID or Enter your user id.

Default Value

This is optional. During playback, whatever you type here appears in the prompt window as the default value but you can change it. If your response to the prompt will usually be the same, type it here.

Is it a Password?

Check this if the input required during playback is a password so that when you type your password, it will be displayed as asterisks. When the macro is saved, the password is encrypted so that it cannot be read.

Clear Host Field

Check this if, during playback, you want the macro to clear the area of the screen in which the information is to be placed before it enters the information. This is useful for host applications that put data into the screen automatically. If such fields are not cleared, invalid characters might be added to the information you enter.



Express Logon



The Express Logon feature allows a user, running a 3270 client session, to log on to a host system without having to enter the user ID and password. One advantage of using this function is that it reduces the time spent by an administrator maintaining host user IDs and passwords. It also reduces the number of user IDs and passwords that users have to remember.

To use Express Logon, the host session must be configured for SSL and client authentication. This means the client must have a valid [client certificate](#). The SSL connection must be made to one of the [supported TN3270 servers](#).

You must first create a macro to log on to the host application and then distribute that macro to the clients. The macro record function steps you through the process for creating an Express Logon macro.

Some configuration needs to be done on the telnet servers and on the z/OS system that you are accessing. The information in these helps describe only what you need to configure for Host On-Demand. Refer to the following telnet server and z/OS documentation for configuration information:

- Communications Server for OS/2 Warp - *What's New*
- Communications Server for Windows NT - *Readme*
- Communications Server for AIX - *Readme*
- Communications Server/390:
 - The following information APARs:
 - II12362 V2R10: IP Configuration Guide (SC31-8725-00)
 - II12363 V2R10: IP Configuration Reference (SC31-8726-00)
 - II12364 V2R10: IP Quick Reference (SX75-0121-04)
 - II12365 V2R10: IP User's Guide (GC31-8514-04)
 - II12366 V2R10: IP Diagnosis Guide (SC31-8521-04)
 - II12369 V2R10: IP Messages Volume 3 (SC31-8674-05)
 - II12370 V2R10: IP and SNA Codes (SC31-8571-04)
 - [OS/390 IBM Communications Server Express Logon User's Guide](#)
 - [OS/390 IBM Communications Server IP Migration V2R10](#)

Related topics:

- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Before configuring Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Distributing an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)

Telnet servers that support Express Logon

Express Logon is supported on the following servers. Refer to the product documentation for configuration information.

- Communications Server for AIX V6.0.0.1 with APAR IY19871
- Communications Server for OS/2 V6.1 with APAR JR16019
- Communications Server for Windows NT V6.1.1 with APAR JR16009
- Communications Server for OS/390 V2R12
- Communications Server for OS/390 V2R10 with APAR PQ47742

and with the following active components:

- VTAM - provides the SNA transport
- TCPIP - provides the TCP/IP transport
- RACF - provides general security services and services for digital certificates and passtickets
- DCAS - TCP/IP application server, which supports the Express Logon function and interfaces to telnet 3270 (middle tier) servers that also support Express Logon.

The TN3270 server and the host must be network connected via SNA and TCP/IP. Refer to [OS/390 IBM Communications Server Express Logon User's Guide](#) for more information.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Before configuring Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Distributing an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)

Changing macro properties



The Macro tab contains properties that apply to the entire macro.

1. Click Macro Manager on the toolbar.
2. Select the macro from the list.
3. Click Edit.

Macro Name

Name of the macro (selected from the list of macros in the Macro Manager).

Description

Description of the macro. Use a description that will help you identify the purpose of the macro.

Author

Name of the person who created this macro.

Creation Date

Date the macro was created.

Pause between Actions

Time to wait between actions associated with a screen defined inside the macro after the screen has been displayed. If this option is not checked, there is no pause between actions. To override the pause time for a specific screen, provide a value for Set Pause Time on the Screens tab.

Timeout between Screens

The maximum time allowed between valid screens while the macro is running. If the time expires before the macro identifies the next screen, an error is displayed. The time set here can be overridden for a specific screen by the Timeout value on the Links tab.

Show all Prompts at Start of Macro

If there are prompts for the user to provide input, checking this option displays all of them at the beginning of the macro. This allows the macro to play through without stopping for input.

Use Variables and Arithmetic Expressions in Macro

Select Use Variables and Arithmetic Expressions in Macro if you want to use variables and arithmetic expressions in your macros. The first time you select Use Variables and Arithmetic Expressions in Macro, a window appears giving you the option to convert your macro to the advanced format (variables and arithmetic expressions).

If you click Yes, your macro is converted to the advanced format. The following changes occur to any field in the Macro Editor where you can type text, a variable, or an arithmetic expression except the Macro tab and the Screen name field:

- String values are enclosed in single quotes ('). For example, an input action with String value hi changes to 'hi'.
- If the String value already contains a single quote, a backslash precedes the single quote. For example, john's changes to 'john\'s'.
- If the String value already contains a backslash, an extra backslash precedes the backslash. For example, ab\c changes to 'ab\\c'.
- The characters +, -, *, /, %, >, <, =, & and | are evaluated as operators unless enclosed in single quotes (') as part of a literal string.
- The characters \$x\$ identify a variable or method (where x is the variable's name, such as \$MyVariable\$) unless enclosed in single quotes (') as part of a literal string.

If you click No, your macro is not converted. Click No if you already converted your macro by editing the macro code, or you want to convert your macro by editing the macro code yourself. If you want to convert your macro yourself, select Edit Code and set usevars to true.

If you deselect Use Variables and Arithmetic Expressions in Macro, your macro might not work as expected if it has been

converted to the advanced format (variables and arithmetic expressions). In this case, Use Variables and Arithmetic Expressions in Macro should remain selected, or you can change the macro code back to its preconverted state yourself, where:

- The single quote and backslash characters are not treated specially. For example, `C:\myfile.txt` writes `C:\myfile.txt` to the screen and `it's` writes `it's` to the screen.
- The characters `+`, `-`, `*`, `/`, `%`, `$`, `>`, `<`, `=`, `&` and `|` are evaluated as literal characters, not operators.

The default is not selected.

For more information about variables and arithmetic expressions, see the online help for [Variables](#) and the *Host Access Beans for Java Reference* in the Host On-Demand Toolkit.

Related topics

- [Using the Macro Editor \(an overview\)](#)
- [Editing the XML script](#)
- [Importing a macro](#)
- [Exporting a macro](#)

Variables

Lists the variables created in this macro. Variables are global to all screens in this macro and any chained macros.

You can assign an arithmetic expression to a variable as the initial value, for example, $2 + 3 + 'a' = '5a'$ or $(5 + 3) * 8 = 64$. Arithmetic operations can be performed on numbers, integer variables, double variables, field variables, and string variables. When your operands are non-numeric, for example, strings and booleans, you can only use the plus sign (for string concatenation). Host On-Demand macros support the following operations:

Symbol	Operation
+	Add
-	Subtract
*	Multiply
/	Divide
%	Mod

For more information about arithmetic expressions, see the *Host Access Beans for Java Reference* in the Host On-Demand Toolkit.

Variables

Lists the variables created in the macro.

Remove

Click Remove to remove the selected variable from the list.

Name

The variable name. A variable name should have the following format: $\$var_name\$$, where *var_name* can be alphanumeric, the dash symbol, and the underscore symbol. Variable names must be enclosed in dollar signs. Variable names are case sensitive.

Type

Select the variable type. Valid values are: string, integer, double, boolean, and field.

The field variable allows you to store the text at a specific row and column on the screen into a variable. If you select field, the Initial Value field is disabled.

Initial Value

Specify the initial value for this variable. The initial value must match the type. The following table lists the variable types and their corresponding values.

Variable type	Value	Examples
boolean	boolean values	true, false
integer	integer number	5, -3, 0
string	text strings; can be a combination of boolean, integer, double, string, field variables, and actual text strings	'hello13' + 5
double	double-precision number	4.2, 1.0e4, -4.8e-3

Variables are created in the macro in the order that they are listed. If the initial value you specify for the current variable is an expression containing other variables, those other variables must appear in the list before the current variable.

Related topics

- [Using the Macro Editor \(an overview\)](#)
- [Editing the XML script](#)

- [Importing a macro](#)
- [Exporting a macro](#)

Obtaining certificates for client authentication

Certificates can be obtained from one of the following:

- [Certificate Authority \(CA\)](#)

Create a client certificate request. After receiving the certificate, export it to a password-protected PKCS12 file and send the password and the file to the user. Make sure the file is securely sent. If a non-secure protocol such as e-mail, http, or ftp is used to send the file over the Internet, the certificate's security can be compromised.

- [Self-signed certificate](#)

You can do this while you are waiting for a CA's certificate, which can take some time. If you think the self-signed certificate provides adequate security, you can use it permanently.



For performance reasons, limit the use of this option. Validation of self-signed certificates can significantly degrade a server's performance.

A Certificate Wizard is provided that creates certificate requests and self-signed certificates, and stores certificates in a client key database. Certificate requests can be made on the Host On-Demand server or locally-installed clients.

Using a browser certificate

Users who currently have a certificate for their browsers can use it directly, or they can export the certificate into a PKCS12 (.p12 or .pfx file type) file format and save it on their workstations to be used for client authentication. Optionally, the certificate can be stored on specialized external media, such as a smart card.

Certificates exported from an older browser are usually weakly encrypted. Use strong encryption when accessing certificates over the Internet with an unsecure protocol, such as http or ftp. To change the encryption strength:

1. Click Communication > Security.
2. Click Show Client Certificate.
3. Locate the certificate and enter the current password.
4. Click View Certificate.
5. Click Settings.
6. Type the current password, and choose Strong for Encryption Strength.
7. Click OK.

Creating a client certificate request

Some CAs have Web pages that you can access for requesting certificates. That is the easiest way to obtain a client certificate.

To create a request:

Certificate Wizard

1. Click Start > Programs > Host On-Demand > Administration > Certificate Wizard.
2. Click Create a Certificate Request and follow the directions provided.

Certificate Management

1. On a Windows server, click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. On an AIX server, enter CertificateManagement from a command prompt. The default location of the AIX script is /usr/opt/hostondemand/bin. Please refer to [Running Certificate Management on AIX](#) for additional information.

3. Create a HODClientKeyDb.kdb database.
4. Follow the instructions in the Help to create the certificate request.
5. Exit Certificate Management.
6. Send the certificate request to the CA.

Sending the certificate request to the CA

Access the CA's Web site and then follow the instructions to request the certificate. Here are the URLs of two 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 or incorporate the request into the form or file provided by the CA. If you need the CA's root certificate, you can often get it directly from the Web site.

While you are waiting for the CA to process your certificate request, you can [create a self-signed certificate](#) to use.

Receiving the certificate

When you receive the certificate, make sure that it is in armored-64 or binary DER format. Only certificates in these formats can be stored in the key database. The Certificate Wizard and Certificate Management programs can only accept simple certificates. They cannot accept certificate chains or PKCS7 data. The armored-64 form of a simple certificate starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----".

To receive the certificate:

Certificate Wizard:

1. Click Start > Programs > IBM Host On-Demand > Administration > Certificate Wizard.
2. Select Import a Certificate and follow the directions provided.
3. Send the certificate and password to the user.

Certificate Management:

1. Click Start > Programs > IBM Host On-Demand > Administration > Certificate Management.
2. Add the certificate to the key database, HODClientKeyDb.kdb.
3. Export the certificate into a password-protected PKCS12 (.p12 file type) file. Send the certificate and password to the user.

Make sure the certificate is securely sent. If a non-secure protocol such as e-mail, http or ftp is used to send the file over the Internet, the certificate's security can be compromised.

A certificate can be stored anywhere on the client's computer, on a diskette, or on a Web server.

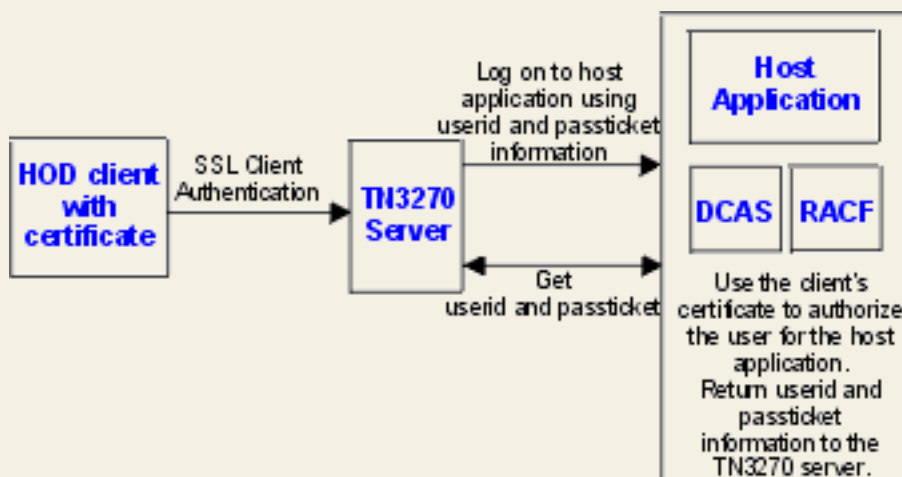
Related topics

- [Client authentication](#)

Using Express Logon

When starting a session using Express Logon, the client establishes an SSL client authentication session with the tn3270 server. During the logon process, a macro with the Logon Express information is played. Once the session is established, the Host On-Demand client sends the application ID for the application that the user is accessing to the tn3270 server. This information is contained in the logon macro. The tn3270 server uses the client's certificate information from the SSL connection and the application ID received from the client, and requests the user ID and passticket (a temporary password) from the host access control program (such as RACF).

The Host On-Demand client uses the macro function to put predefined substitute strings in the user ID and password fields. The tn3270 server substitutes the user ID and passticket in the appropriate place in the 3270 datastream. The logon is completed.



Related topics:

- [Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Before configuring Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Distributing an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)

Before configuring Express Logon



Before you configure an Express Logon macro, you need to have the following information available:

- **Host application name**
Name of the host application the user is logging onto. For example, the name entered on the USSMSG10 screen.
- **Host access application ID**
This name must match the RACF PTKTDATA (Passticket Data Profile) application name that is configured on the OS/390 V2R10 host. This name could be the same as the application name that the user is logging onto (for example, the name on USSMSG10). When creating PTKTDATA profiles for applications such as TSO, the application name portion of the profile will most likely not be the same. For example, RACF requires that the application ID portion of the profile name be TSO+SID. Refer to OS/390 V2R10.0 SecureWay Security Server RACF Security Administrator's Guide to determine the correct profile naming. If using TSO Generic Resource names, RACF apar OW44393 is needed.
- **Alternate start screen**
A start screen is the first screen from which the macro is played. In addition, one or more subsequent screens can be designated as an alternate start screen. Alternate start screens should be identified during the recording process so that the macro can be played from those screens. For example, when the 3270 Host On-Demand session is started, you might see a USSMSG10 screen. On that screen, you enter the host application name (for example, TSO or MVS) and then go to the application's logon screen. The application logon screen could be identified as an alternate start screen. You can play the macro from either the start screen (USSMSG10) or the alternate start screen (application logon screen). You can not designate an alternate start screen once the user ID has been recorded.
- **User ID and password**
User ID and password for the application to which you are logging on. During macro recording, the actual user ID and password are used. They are not recorded in the macro, only the predefined substitute strings are recorded in the macro. The tn3270 server replaces the predefined substitute strings with the actual user ID and password during the logon process.
- **Certificate**
The workstation certificate must be stored in RACF using the RACF RACDCERT command.
 - For information about using digital certificates with RACF, refer to the OS/390 V2R10.0 SecureWay Security Server for OS/390 (RACF) Security Administrator's Guide and the OS/390 V2R10.0 SecureWay Security Server for OS/390 (RACF) Command Reference.
 - For information about configuring DCAS to use RACF certificates, refer to the OS/390 V2R10.0 IBM CS IP Configuration Guide.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Distributing an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)

Configuring Express Logon



To configure Express Logon, you must record a macro for each host application that you want to access. You cannot log on to multiple applications with one macro. SSL configuration and client authentication on the telnet servers and z/OS is not required before recording the logon macro but must be done before you can play the macro.

To configure a session for Express Logon:

1. [Create a 3270 display session](#) for the administrator user.
2. Load the Host On-Demand client, logon as the administrator, and start the session you created in Step 1.
3. Make sure you are at the start screen of the host application before you start recording. This should be the logon screen or the one before it. **Do not log on.**
4. Record a logon macro. Click Record Macro on the Macro toolbar. Type a name and description for the macro. Use a name that will help you to recognize it as an Express Logon macro.
5. Check Express Logon Feature.
6. Enter the application ID. This is the host access control facility's application ID.
7. Continue through the Express Logon macro recording. Click Help if you need more information. 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. Click Stop Recording when you have completed the recording of all the screens.
9. Enable SSL and [client authentication](#). Right-click the session icon, select Properties, and then click the Security tab.
10. Test the macro. Click Play Macro on the Macro toolbar.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Before configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Distributing an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)

Recording multiple user IDs for an Express Logon macro

To record multiple user IDs:

1. Click Record Macro on the Macro toolbar.
2. Check Express Logon Feature.
3. Enter the Application ID.
4. Continue with the logon. Enter the first user ID or password on the session screen.
5. Use the Express Logon macro to complete the recording including the second, or last, user ID or password.
6. [Edit the macro](#) using the Macro Editor.
7. Click the Macro tab, select the macro you just recorded and click Edit Code.
8. Find the XML input value tag that contains the user ID that you entered on the screen in Step 4 and replace it with ")USR.ID(" string.
9. Click Save.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Configuring Express Logon](#)
- [Distributing an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)

Distributing an Express Logon macro



There are two ways you can distribute the macro once it's created:

- Export the macro to a file and distribute the file to your users (click Export in the Macro Editor window). Users then import the macro for their session (click Import in the Macro Editor window).
- [Export the 3270 session](#) that was configured with the Express Logon feature, from the Host On-Demand client to a file. Start the Host On-Demand Administrator and create a group. [Import the 3270 session](#) to the group.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Before configuring Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Express Logon problem determination](#)



Express Logon macro limitations



Limitations of the logon macro:

- If the position of the user ID and password fields on the logon screen change, the macro must be re-recorded.
- There is a short delay while the tn3270 server acquires the passticket from the host access control facility. The amount of time is probably less than the usual delay incurred when the user enters a user ID and password. However, the user can see the macro proceed through the screens during the logon process.
- The Logon Express macro can record the user ID and password on one screen only. [If you need to record the user ID or password on multiple screens, then you must record it on the session window, not through the Express Logon window.](#)
- If you are connecting to a tn3270 server through a [Redirector](#), the security option for the Redirector configuration must be set to Pass-through.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Before configuring Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Distributing an Express Logon macro](#)
- [Express Logon problem determination](#)

Express Logon problem determination



If the client logon fails and displays the message ")USR.ID(NOT IN CP DIRECTORY", "INVALID USERID,)USR.ID(", "PASSWORD NOT AUTHORIZED" or any similar messages, check the tn3270 server log for details. Possible reasons for failures are:

- The application ID defined in the macro is not valid.
- The tn3270 server could not connect to DCAS. The host might be down.
- The client certificate is not defined in RACF or it is not valid.
- The passticket has expired and could not be used to log on.
- The tn3270 server completed scanning of data stream without replacing the user ID or password.
- The tn3270 server or the host does not support the Express Logon Feature.

Related topics:

- [Express Logon](#)
- [Using Express Logon](#)
- [Telnet servers that support Express Logon](#)
- [Before configuring Express Logon](#)
- [Configuring Express Logon](#)
- [Recording multiple user IDs for an Express Logon macro](#)
- [Express Logon macro limitations](#)
- [Distributing an Express Logon macro](#)

Exporting sessions



If you are exporting a session icon configured for multiple sessions, you must export 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 export all 3 of those sessions along with the multiple session icon.

To export a Host On-Demand session to a file:

1. In the Configured Sessions area, right-click the icon for the session you want to export, then click Export Session.
2. Type a filename for the exported session, or click Browse. The default file extension is .hod.
3. Click OK.

The parameters for the selected session are saved in this file. You can later import the file to restore a session and you can duplicate the file for distribution.

Using exported sessions

The ability to configure sessions for groups of users provides the administrator with one method of distributing sessions; the Export function provides even more flexibility because it allows administrators to distribute sessions regardless of groups.

For example, if an administrator publishes a session on a Web site, users can download the session and import it. This eliminates the need for administrators to add large numbers of users to a single group to make the session publicly available.

Related topics

- [Importing sessions](#)

Importing sessions

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 3 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:
 - Session files previously created by exporting Host On-Demand sessions
 - Telnet sessions from Personal Communications v4.1 or later
3. Click OK.

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. Features such as screen colors and key mappings may not be correct.

Related topics

- [Exporting sessions](#)
- [Importing Personal Communications printer sessions](#)



Importing Personal Communications 3270 printer sessions

A Personal Communications 3270 printer session can use the normal printer drivers or a printer definition table (PDT). A 5250 session uses the normal printer drivers for both standard and Host Print Transform (HPT) printing; for standard printing, it can also use a PDT.

A Host On-Demand 3270 printer session can use the normal printer drivers or a PDT; a 5250 session always uses HPT without a PDT.

When you import a Personal Communications session, the following conversions are made:

- **3270 sessions that use the normal printer drivers**
These sessions are configured to use the normal printer drivers.
- **3270 sessions that use a Printer Definition Table (PDT)**
The import facility attempts to identify a corresponding Host On-Demand PDT. If an exact match is not found, the new session is configured to use whichever Host On-Demand PDT provides the closest match. If a match cannot be made, the Basic ASCII text mode PDT is chosen.

Sessions that are configured to use Printer Definition Tables (PDTs) are mapped to use the same PDT in Host On-Demand only if the Host On-Demand PDT exists when the session is imported. You may have to work with the users to set this up.

For example, suppose there is a Personal Communications printer session named mySess.ws that uses a PDT named myPD.pdt. Before mySess.ws is imported into Host On-Demand, you must obtain a copy of myPD.pdf, place it on the Host On-Demand server and run the PDT compiler. (See [PDT Compiler](#) for help on compiling PDFs.) This creates the Host On-Demand PDT, named myPD.hodpdt, and also registers the PDT with the HOD server. You can then import mySess.ws, and myPD.pdt will map to myPD.hodpdt on the server.

- **Personal Communications 5250 sessions that use standard printing and the normal printer drivers**
These sessions are configured to use HPT and the IBM 4201-1 Proprinter.
- **Personal Communications 5250 sessions that use HPT**
These sessions are configured to use HPT and the printer that most closely matches the Personal Communications printer. If a match cannot be made, the IBM 4201-1 Proprinter is chosen.
- **Personal Communications sessions that use standard printing and a PDT**
These sessions are configured to use HPT and the printer that most closely matches the Personal Communications PDT. If a match cannot be made, the IBM 4201-1 Proprinter is chosen.



Host On-Demand services



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.

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 [OS/400 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:

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.

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

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).

Click OK to start the service manager trace. The trace status and trace level remain the same across Service Manager starts and stops.

Using the Host On-Demand Redirector



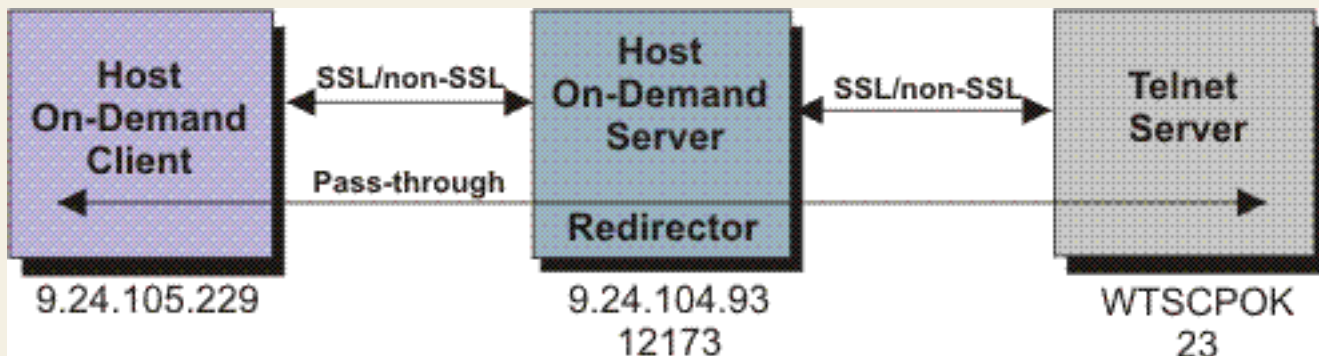
- [Adding a host](#) to the Redirector.
- [Changing the session configuration](#) to connect to the Redirector instead of the host.
- [Setting up Redirector with SSL](#).

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 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 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.



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).



Configuring an OS/400 proxy



server

To use a proxy server, you must enable the proxy server on the Host On-Demand server. One advantage of using a proxy server is that only one port is opened through the firewall when transferring files to an iSeries system. All the data flows through the specified configured port. The default port is 3470. When a proxy server is not enabled, multiple ports are used.

To configure an OS/400 proxy server:

1. Click Services in the Administration window.
2. Select OS/400 Proxy Server.
3. Click Yes to enable a proxy server.
4. Enter a server port and a maximum number of connections.
5. Click Apply.

Limitations

- When SSL is enabled, server authentication is used for encrypting data between the client and the host for transferring files to an iSeries. However, if you enable both SSL and a proxy server, encryption is done only from the proxy server (Host On-Demand server) to the host (iSeries): data is **not** encrypted on the client side (from the client to the proxy server).
- If you are trying to avoid opening any ports on the firewall by using the configuration servlet, you still must enable the configured proxy server port for 5250 file transfer and Database On-Demand.
- Transferring SAVF type of files is not supported with the proxy server enabled.

Related topics

- [Using Database On-Demand](#)



Adding a host to the Redirector



To add a host to the Redirector:

1. Click Redirector Service in the Administration window.
2. Click Add.
3. Enter the target host's destination address. Make any necessary changes to the port numbers or security.
4. Click OK to save the connection and add it to the Redirector window.

Destination Address

Enter 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

Enter the port number on the telnet server through which it will communicate with the Redirector. Many hosts use the default, which is 23, for Telnet connections.

Local Port

Enter 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 numbering scheme, use port numbers that are not already defined for other TCP/IP applications. Because most well-known port numbers are less 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 for each host configuration. The choices are:

- Pass-through - no modification to the data stream between the client and host
- 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
- Both - provides encryption of data transmitted, through the Redirector, between the emulator and a secure server

If you are using the [Express Logon Feature](#), this option must be set to Pass-through.

Related topics

- [Redirector overview](#)

Configuring a session to connect to the Redirector

1. Click Add Sessions at the bottom of the Host On-Demand window.
2. Right-click the icon for the type of session you want to add.
3. Click Copy.
4. Enter the Destination Address for this session. This is the host name or IP address of the Host On-Demand server on which the Redirector is running.
5. Enter the Destination Port for this session. The port number should be the same as the Local Port number defined in the Redirector for the host you are connecting to. Each host configured in the Redirector has a different port number. The default for 3270, 5250 and VT connections is 23. The default for CICS connections is 2006.
6. Enable Security (SSL) if necessary. If you enable it, be sure that the Redirector has enabled client-side security for this connection. Click the Security tab and then click Yes for Enable Security.
7. Click OK.
8. Click Close to close the Add Sessions window.
9. Double-click the session icon to start the session.

Session configuration example

In this example, a host connection is added to the Redirector running on a Host On-Demand server with the host name hodserver:

Destination Address

RALVM13

Destination Port

23 (default)

Local Port

12173 (assigned when you add a host connection)

Security

Client-side (for secure sessions)

Your session configuration will then use these values:

Destination Address

hodserver (the host name of the server in which the redirector service is running).

Destination Port

12173 (Local Port number assigned above)

Related topics

- [Redirector overview](#)
- [Adding a host to the Redirector](#)
- [Setting up Redirector with TLS or SSL](#)



Setting up Redirector with TLS or SSL



To set up Host On-Demand Redirector with TLS or SSL using a Self-Signed Certificate, do the following:

1. Use Certificate Management to create a new CMS key database file. For example, HODServerKeyDb.kdb.
2. Type a password for the key database file, and make sure you select to store the password to a file.
3. Select Personal Certificates from the drop-down menu.
4. Select Create a New Self-Signed Certificate.
5. Extract the certificate as a Base64 .arm file to /hostondemand/bin.
6. Create an SSLight key database class. For example, CustomizedCAs.class in /hostondemand/HOD.
7. Select Signed Certificates from the drop-down menu and add the .arm certificate file. Label the certificate appropriately.
8. Restart the Host On-Demand Service Manager.
9. Modify or add a Redirector Service with client-side security.
10. Modify or add a session to connect with the TLS or SSL-enabled Redirector Service.

Enabling TLS or SSL tracing in the Redirector code

To enable TLS or SSL tracing in the Redirector code, follow these steps on the system running Redirector:

1. Stop the Service Manager if it is currently started.
2. Set an environment variable:

```
SVR_START_TRACE =Yes
```

To set this variable:

- o For Windows NT, Windows 2000, and Windows XP use the GUI.
- o For Windows 95 and 98, use set command on a command line.
- o For AIX, use the export command.

Note: The variable value is case sensitive.

3. Start the Service Manager. Under the ..\hostondemand\private directory, look for the file named NativeSSLTrace.trc. This file has the trace data from the Redirector.
4. To stop the trace, stop the Service Manager and set the value of the environment variable to No. Delete the NativeSSLTrace.trc file if necessary.

Note: Each time the Service Manager is started, the trace file is newly created. All existing contents of the file are overwritten.

Resolving Redirector Problems

Following are several techniques that might be useful in resolving Redirector problems:

1. Turn on HOD Debug Trace. This is helpful for IBM Support.
 1. Turn on trace debug level to enhance the Host On-Demand trace that is normally captured in NCoDServices.RAS.txt file. This file is very useful to IBM technicians when they are trying to resolve Host On-Demand problems.
 1. For Windows Server, run regedit to edit the registry; add the following /d3 parameter to the appropriate line in the registry. The key to modify is:

```
HKEY_Local_Machine
    System
        CurrentControlSet
            Services
                IBMSERVICEManager
```

Add this to the end of the /d3 line in the parameters section of this key in the KEY AppParameters. There must be a space between the last character of the line and the /d3.

The following registry entry shows the value of the registry being accessed(controlset001 or 002) or the current controlset:

```
HKEY_Local_Machine
    System
        Select
```

2. For AIX servers, edit the shell script that starts Host On-Demand, and add the following /d3 as indicated. You can add the /d3 in

multiple places, depending on which Debug option you want to use. Here are two examples from the shell script that ships with Host On-Demand:

```
# This line is with JIT off and error logging on
# java -Djava.compiler=off -classpath
.:sm.zip:ibmjndi.jar:jndi.jar:jsdk.jar:ods.jar:$CLASSPATH
com.ibm.eNetwork.HODUtil.services.admin.NCServiceManager
/usr/lpp/HOD/hostondemand /d3
```

```
# This line is with JIT on and error logging on
# java -classpath
.:sm.zip:ibmjndi.jar:jndi.jar:jsdk.jar:ods.jar:$CLASSPATH
com.ibm.eNetwork.HODUtil.services.admin.NCServiceManager
/usr/lpp/HOD/hostondemand /d3
```

Save NCoDServices.RAS.txt for IBM support to examine.

2. Search for javacore*. * files. Save these files for later use by IBM support.
2. Verify that there is network connectivity for the Host On-Demand Redirector.
 1. From the computer that is running the Redirector, ping the host system to which you are trying to connect your emulator sessions. If the host is known to respond to pings, and the ping fails, there is connectivity failure on the network; however, not all hosts respond to pings. For example, if your telnet host is called RALVM17, at a command line type: **ping RALVM17**.
 2. Try opening a Host On-Demand session that is configured to connect directly to the host, bypassing the Host On-Demand Redirector. You might need to ask your Host On-Demand Administrator to configure a session with these properties. This might not be possible because it depends on the ports and TLS or SSL settings for your host computer. If the direct-connection session works, this implies that there is a problem on the computer running the Redirector. The problem can be with the Redirector itself or with connectivity from the computer where the Redirector is running to your host. If you have a firewall between the Redirector and host computer, ensure that the open firewall ports correspond to the destination port configured for Host On-Demand Redirector redirected session. If the computer where the Redirector is running is in your network DMZ, ensure that the DMZ allows the Redirector to connect to the host systems.
3. Try one of the following:
 1. Start a Host On-Demand session that is not configured to use the Redirector, and connect directly to the host system on the machine running the Host On-Demand Redirector. If this does not work, there might be a failure of the host listening for a connection. If this works, and step two also works, there might be a problem with the Redirector. If this is the case, call IBM service. Be sure to compare the settings in the session that does connect to the Redirector configuration with the destination address for the redirected session with which you have problems.
 2. If your host connection does not use TLS or SSL, try setting up a windows Telnet session. From the machine running the Redirector, at a command prompt, type:

```
telnet <hostname> <portno>
```

Note: On Windows NT, a port default of 23 is used instead of the <portno> parameter. To specify a port other than 23, type:

```
telnet
```

Then, specify the correct hostname and port number on the telnet GUI that is displayed.

There are different variations of telnet for different host types, but you will at least see if the telnet command is successful. If this works and step two also works, there might be a problem with the Redirector. In this case, call IBM service. Be sure to compare the settings in the session that does connect to the Redirector configuration with the destination address for the redirected session with which you have problems. If this does not work, the problem might be with a firewall or with a setting on the host system.

4. If the previous steps fail, go to a Windows command prompt and type **nslookup x.y.z.w**, where **x.y.z.w** is the dotted-decimal address of the host system. If nslookup cannot resolve the dotted-decimal address to the host name of the host to which you are connecting, there is a problem with the DNS on your network. One way to avoid this problem is to add the hostname and its IP address to the HOSTS file on the computer running the Redirector. For Windows, the HOSTS file is located in WINNT\system32\drivers\etc. The file looks similar to this:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names.
# Each entry should be kept on an individual line. The IP address
```

```

# should be placed in the first column followed by the
# corresponding host name.
# The IP address and the host name should be separated by at least # one space.
#
# Additionally, comments (such as these) may be inserted on
# individual lines or following the machine name denoted by a '#'
# symbol.
# For example:
#
#           102.54.94.97      rhino.acme.com      # source server
#           38.25.63.10      x.acme.com        # x client host

127.0.0.1      localhost
9.27.118.9     hodServer

```

3. If you have configured the Redirector for TLS or SSL, verify the TLS or SSL configuration.

1. If host security is on, verify that the host telnet can do TLS or SSL.
 1. If the Redirector port is set to client security, the TLS or SSL server in respect to the client is the Host On-Demand Redirector, and not the final telnet server to which the client is going.
 2. If the Redirector is doing TLS or SSL security between the Redirector and the host server by setting the Redirector port to host security, the client configuration must set security no. This is because the data between the host and the Redirector is encrypted, but the data between the Redirector and the client is not encrypted.
2. Ensure that CustomizedCAs.class and the HODServerKeyDB.* contains security certificates that have not expired. Use the CertificateManagement tool that comes on Windows and AIX platforms to verify valid security certificates. Open the key databases and click on the personal certificates, then view them. The validity period information is listed in the window that appears. Unfortunately, Host On-Demand does not have built-in support for CRLs, so the expired certificates are not flagged or removed automatically.
3. Run HODRemove.html on the computer running the Host on-Demand client, in case the client has at any time used cached client.
4. Verify that the HODServerKeyDb.* files are present in the \hostondemand\bin directory. This is the key database file that is used by the Host On-Demand Redirector; It contains certificates from well-known CAs. It also contains the private key and any personal certificates for the server.
5. If you are using a self-signed certificate, verify that CustomizedCAs.class is present in the \hostondemand\HOD directory. If you are using a self-signed certificate or a certificate issued by an unknown CA, the certificate must be extracted and included in the CustomizedCAs.class file. This file is located in the Host On-Demand publish directory so that the clients can get to it. It is downloaded every time the Host On-Demand client is downloaded.
6. Ensure that the service manager is stopped and restarted each time the .kdb file or the CustomizedCAs.class file is created or updated.

Related topics

- [Using the Host On-Demand Redirector](#)
- [Configuring a Session to Connect to the Redirector](#)
- [Adding a host to the Redirector](#)



Changing a host defined to the



Redirector

To change a host that has been defined to the Redirector:

1. Click Redirector Services Administration window.
2. Highlight the host configuration you want to change.
3. Click Change.
4. Make the necessary changes.
5. Click OK to save your changes.

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)

Related topics

- [Redirector overview](#)
- [Adding a host to the Redirector](#)
- [Deleting a host from the Redirector](#)



Deleting a host from the Redirector



To delete a host from the Redirector:

1. Click Redirector Service in the Administration window.
2. Select the host configuration you want to delete in the Redirector window.
3. Click Delete, then confirm.

Related topics

- [Redirector overview](#)
- [Adding a host to the Redirector](#)



Enabling license usage counting



To view information about license usage or enable usage counting, click Licenses in the Administration window. Information from the latest count is displayed when you open the License window or when you click Refresh.

License Use Statistics

This information applies only when clients are reporting to this Host On-Demand server. Refer to the License Use Management server documentation about reviewing statistical information for clients reporting to a License Use Management server.

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.

License Use Count

Configure the Host On-Demand server so that clients downloaded from this server report to a Host On-Demand server or a License Use Management server.



You must click Apply to activate any changes that you make.

Enable

Enables clients downloaded from this server to report to a Host On-Demand server or to a License Use Management server. To stop clients from reporting to a server, clear the check box.

Clients Report to

Select whether you want clients to report to a Host On-Demand or a License Use Management server.

Host Name/IP Address

Type the host name of the Host On-Demand or License Use Management server that clients must report to.

Report Interval

Select the amount of time for clients to wait between reports. Clients begin using the new interval once the previous interval has expired.

Related topics

- [Considerations for selecting a report interval time](#)
- [License usage overview](#)



Considerations for selecting a



report interval

Choose the smallest value possible for the report interval. This provides the most accurate count of concurrent users and, for most users, does not create any performance problems in terms of network traffic or server CPU usage.

If you are not sure what report interval to choose, the following considerations might help you to decide:

- In most cases, set the report interval to a value that is less than the average amount of time that the typical user is connected to the Host On-Demand server. If your server has plenty of bandwidth or if you do not have many sessions running concurrently, this is your only consideration and you should set the report interval to the minimum value allowed.
- If your network is severely constrained for bandwidth or your Host On-Demand server is constrained by its processor, you might want to increase the report interval time. Each client workstation that downloads and uses any part of Host On-Demand provides a check-in signal to the server once at each report interval. The longer the interval, the less network and server traffic is generated.

At the end of each report interval, the Host On-Demand server counts all the workstations that have reported. The reports and the CPU resources required to count the number of workstations are very small.

- Any client recognized at the report interval is recorded as having accessed the Host On-Demand server at some point during the report interval, even though the client is no longer connected when the count is made.



License Usage



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. A License Use Management (LUM) server enables you to manage and control licenses for Host On-Demand and other software products.

Choose the server that you want clients to report by clicking Licenses in the Administration window. Clients can be switched to report to either type of 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.



If you are using a License Use Management server, import the license file **liblicusemgmt.lic** to the LUM server using the Basic License Tool. Refer to the LUM product documentation for overview and configuration information.

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.

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 LUM or HOD.
- The identity of the License Use Management server. The property name is defined by the constant `ECLSession.SESSION_LUM_SERVER`, and the value must be the host name or IP address of the License Use Management server.
- The port number of the License Use Management server. The property name is defined by the constant `ECLSession.SESSION_LUM_PORT`.
- 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 `userid`, and the value must be a string that uniquely defines a user in a multi-user environment.

If you are using AIX as the License Use Manager (LUM) for Host On-Demand, the Basic License Tool (BLT) of the LUM might terminate abruptly, and you won't be able to restart it if there is an active Host On-Demand client with the user profile "default" using a Netscape browser. In order to restart the BLT, stop the Host on-Demand session on the client, close the browser, and delete the "Users" subdirectory in the Netscape directory. Then start the Netscape browser again on the client and define a user profile other than "default". You can then restart the BLT of the AIX LUM, and it will operate correctly.



Related topics

- [Enabling license usage counting](#)
- [Considerations for selecting a report interval time](#)

Getting started with Database On-Demand

The Database On-Demand client lets you extract data from an iSeries database for use in a client workstation application, and upload files created on the client to the iSeries database.

To start Database On-Demand:

1. Load the Database On-Demand client, HODDatabase.html, into a browser.
2. Type your user ID and password for the Host On-Demand server that you are accessing.
3. Click Log On.

When the client window opens you are presented with two tabs:

- The SQL Wizard tab
The SQL Wizard tab is the default view. It displays a view of previously saved SQL statements. You can open, run and delete existing SQL statements, and create new SQL statements.
- The File Upload tab
This tab displays a view of previously saved File Upload statements. You can open, run and delete existing File Upload statements, and create new File Upload statements.

[Creating a new SQL or File Upload statement](#)

[Opening an existing SQL or File Upload statement](#)

[Running an existing SQL or File Upload statement](#)

[Deleting an existing SQL or File Upload statement](#)

If you are loading the Database On-Demand client on a UNIX operating system, and you cannot see the logon text you enter, try changing the color of the desktop:

1. Start the application Desktop Style from the toolbar.
2. Start the application Colors and select a different color setting.

Creating a new SQL or File Upload statement

To create a new SQL or File Upload statement and save the statement for later use:

1. Click New. The logon tab displays.
2. Type the URL for the iSeries database:

```
jdbc:as400://iSeriesname
```

To use SSL when connecting:

```
jdbc:as400://iSeriesname;secure=true
```

To use a [proxy server](#) when connecting to the iSeries database, include the proxy server name and port number:

```
jdbc:as400://iSeriesname;proxy server=HODServerName:proxyServerPort
```

3. Type your user ID and password (if required) for the database.
4. Select the JDBC driver you want to use to access the database. (See [Logon tab](#) for more information for this tab.)
5. Click Connect to connect to the database.

6. Once you are connected, a series of new tabs appears at the top of the Logon tab. The tabs that appear depend on whether you are creating a new [SQL statement](#) or a new [File Upload statement](#).
7. When you are satisfied that the SQL statement is correct, click Save SQL on the SQL tab to save the statement. Or, when you are satisfied that the File Upload statement is correct, click Save statement on the File tab to save the statement. Once saved, the SQL or File Upload statement appears as an entry on the appropriate Database On-Demand tab for later use.



If you have Java 2-enabled browsers, you must press and hold the Ctrl key while selecting multiple table names.

Opening an existing SQL or File Upload statement

You can view and edit the options used to create an existing SQL or File Upload statement. This allows you to make changes to commands without reconstructing them each time. For example, if you are running an SQL statement that pulls all the payment records received for the current month, you might want to change the month options in the SQL statement at the beginning of each month. If you open and edit your existing SQL statement, you do not have to build a new SQL statement each month.

To open an existing SQL or File Upload statement:

1. Click the icon for the SQL or File Upload statement that you want to open.
2. Click Open.
3. The logon tab displays. If necessary, fill in the required information and click Connect.
4. Once you are connected, a series of new tabs appears at the top of the Logon tab. These tabs contain either your original [SQL statements](#); or your original [File Upload](#) statements. You can change the supplied information, execute the new SQL and save the results, or run the new File Upload statement.

Running an existing SQL or File Upload statement

To run an existing SQL or File Upload statement:

1. Click the icon for the SQL or File Upload statement you want to execute.
2. Click Run.
3. Enter your ID and password (if they were not saved with the selected SQL or File Upload statement). Type the information and click Connect. If you saved the ID and password with this SQL or File Upload statement, skip the next step.
4. Either your SQL statement results are displayed or sent to a file (see [Output tab](#) for more information); or you File Upload statement uploads the file to the host database.

After running the SQL or File Upload statement, you can modify it by changing one or more of the options on the various tabs. Click Run SQL on the SQL tab to rerun the SQL statement, or click Run statement on the File tab to rerun the File Upload statement.

Deleting an existing SQL or File Upload statement

You may need to remove SQL or File Upload statements that have been previously saved. You can delete an existing SQL or File Upload statement but remember that once statements are deleted they cannot be recovered; you must build a new statement.

To delete an existing SQL or File Upload statement:

1. Click the icon for the SQL or File Upload statement you want to delete.
2. Click Delete.
3. Click OK.

You must log on as an administrator to delete statements at the Group level.

Related topics

- [Database On-Demand overview](#)
- [Setting Database On-Demand options for users](#)

Database On-Demand SQL statements



Database On-Demand provides an interface for creating, modifying, and running SQL statements. A set of tabs guides you through the process of building and executing a valid SQL statement. The tabs include:

- [Logon](#)
- [Tables](#)
- [Join](#)
- [Condition](#)
- [Columns](#)
- [Sort](#)
- [Output](#)
- [SQL](#)
- [Results](#)
- [Insert](#)
- [Update](#)
- [Delete](#)

Logon

Click the Logon tab to connect to the target database. All fields are required.

- **Database URL**
Type the URL for the database you want to work with. Consult your JDBC driver documentation for the format of the database URL. For example, the iSeries Toolbox for Java JDBC driver requires:

```
jdbc:as400://iSeriesname
```

where *iSeriesname* is the fully-qualified network name of the database host.

To use a [proxy server](#) when connecting to the iSeries database, include the proxy server name and port number:

```
jdbc:as400://iSeriesname;proxy server=HODServerName:proxyServerPort
```

- **Userid/Password**
Type your user ID and password for the specified database.
- **Driver description**
Select the JDBC driver used to communicate with the specified database.
- **Class name**
This field contains the class name of the driver associated with the descriptive name in the Driver field.

Enter the required information and Click Connect to open a connection to the host database.

Note:

- If 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 so that it is not a dll file type and restart your browser. This file is located in the \program files\netscape\communicator\program\java\bin\ directory.
- If you see this message when logging on: Please reset the environment variable CLASSPATH to NULL. you must stop your browser, reset the CLASSPATH to NULL and restart your browser. Check the documentation on your operating system for information regarding how to reset environment variables.

After connecting, the connect button is replaced by a Disconnect button, which allows you to disconnect from the database. Also, the following set of tabs are added to the Logon tab:

Tables

Click the Tables tab to specify the tables you want to access in your SQL statement, and the type of SQL statement that you will generate.

1. Select the SQL statement type you want to use. Valid statement types include:
 - **Select**
Allows you to select records from host database table(s).
 - **Select Unique**
Allows you to select distinct records from host database table(s).
 - **Insert**
Allows you to insert a record into the host database table.
 - **Update**
Allows you to update the host database table records using the given values.
 - **Delete**
Allows you to delete records from the database table, and you can specify a condition for deletion.
2. Select the table(s) you want to access. You can select multiple tables when the statement type is select or select unique.
3. Click Next.

Click View schema(s) to add tables from additional schemas. A schema is similar to a database or library. For iSeries schemas, the defaults are what is in the default library list for the user profile.

Click Refresh to update the list of tables that are displayed. New tables that were added to the schema are displayed in the Table list; deleted tables are removed. Refresh does not reset any selections that have been made.

Join

Click the Join tab to:

- [Join fields from multiple selected tables](#)
- [Join a table alias](#)
- [Remove a join](#)

This tab is used only if two or more tables are selected.

Joining fields

1. Select a column from the first table.
2. Select a column from the next table.
3. Click Join.

A line connects the joined columns and changes color when the join is enabled. Note that the information area keeps you informed of the join status and will let you know if a requested join is not valid. You cannot, for example, join columns with

mismatched data types.

By default, a join request is assumed to be an *inner join*. An inner join joins only the rows where the values of the two columns match. Click Options to request other types of joins. You can select:

- **Left outer join**

This is an inner join that includes any rows in the left-most table that are not already included in the inner join.

- **Right outer join**

This is an inner join that includes any rows in the right-most table that are not already included in the inner join.

When you are working with multiple joins, use the left and right arrow buttons (< >) to navigate between joins. The selected join is indicated by a line.

Joining a table alias

You can join a table column with an *alias* column. An alias is an alternate name for a table. Using an alias allows you to join two columns in the same table, or to create a more meaningful name for the column.

1. Select a column from the table.
2. Click Alias. This creates an alias for the selected table and displays the table columns. The two lists of columns will be the same.
3. Select a column in the alias.
4. Click Join.

Removing a join

1. Select the joined columns.
2. Click Unjoin.

The join line disappears.

When you finish with the Join tab, click Next.

Condition

Click the Condition tab to:

- [Specify one or more SQL conditions.](#)
- [Remove a SQL condition.](#)

Specifying an SQL condition

1. Select the table you want to use from the Selected table(s) drop-down list. The Selected tables(s) list includes only the tables that are selected on the Tables page.
2. Select the column from the Columns list.
3. Select an operator from the Operator list.
4. Specify values. You can type values in the fields, or you can click Find and select from the Value Lookup list. To remove a selected value from the Value Lookup list, click Clear.

The Value Lookup window allows you to find values for a condition.

1. Type a character string in the Search for field and click Find now.
2. Check Case sensitive if you want to search for upper and lower characters exactly as typed in the Search for field.
3. Select a Maximum hits value. This controls the number of values returned for each search.
4. Select a value or values from the list and click Use value.

5. Click OK.

Click Cancel to close the Value Lookup window without adding any of the selected values to the Condition tab.

To specify additional SQL conditions:

1. Click **Find on another column** to display a second condition tab. This tab is labeled Condition 2.
2. Follow the preceding steps to specify the second condition.

Click Find on another column for each additional condition until you have specified all the conditions for the SQL statement.

Removing an SQL condition

Select the appropriate condition tab, then click Delete.

When you finish with the Condition tab, click Next.

Columns

Click the Columns tab to select the columns you want to include in the query results.

1. Select a table from the Selected table(s) drop-down list.
2. Select one or more columns from the Columns list.
 - Click Select all to select all columns in the list.
 - Click Deselect all to deselect all columns in the list.
3. Select Add to add selected columns to the list.

Use the Add<< and >>Remove buttons to move column names from one list to another.

When you finish with the Columns tab, click Next.

Sort

Click the Sort tab to specify the column(s) used to sort the results.

1. Select a table from the Selected table(s) drop-down list.
2. Select one or more columns from the Columns list.
 - Click Select all to select all columns in the list.
 - Click Deselect all to deselect all columns in the list.
3. Select Add to add selected columns to the Columns to sort on list.

Use the Add>> and <<Remove buttons to move column names from one list to another.

You can select Ascending or Descending from the Sort Order field for each of the lines in the **Columns to sort on** list. Columns sorted in ascending order have leading characters of a-through-z; descending order columns have leading characters of z-through-a. Columns are sorted in ascending order by default.

The sort rules apply in the order they appear in the **Columns to sort on** list. The primary sort column is at the top of the list, the secondary sort column is second in the list, and so on, until there are no more lines in the list. If you want to adjust the order in which the sort rules apply, use the following buttons:

- **To make a column's sort order earlier:**
Select the column in the **Columns to sort on** list, then click Move up.
- **To make a column's sort order later:**
Select the column in the **Columns to sort on** list, then click Move down.

When you finish with the Sort tab, click Next.

Output

Click the Output tab to direct the output (results) of the SQL query to your display or to a file.

1. **Display**
Choose Display if you want the output to be directed to the display. The results of the query appear on the Results tab.
2. **File**
Choose File if you want the output to be directed to a file.

When you finish with the Output tab, click Next.

You can specify whether you want the results of the SQL statement directed to the Results tab or to a file. The main selection options are Display or File.

1. **Display**
Directs the output to the display. The query results appear on the Results tab after you run the SQL statement.

You can limit the number of rows displayed on the Results tab by adjusting up or down the **Display Options - Maximum number of rows to display** field. The maximum number of rows that can display is 1000. If you have queries that generate more than 1000 rows, it is recommended that you direct the query output to a file rather than to a display. If the query generates more rows than the maximum specified in this field, the additional rows are ignored.

2. **File**
Directs the output to a file.

Several fields are required when you save the results to a file.

- **File name:**
Specify the file name, a drive and a directory path name for the target file. Click Browse to select a file name, a path name, and a drive, if you desire.
- **File Type:**
Select the format for the stored results.
 - **ASCII Text**
Stores the results in plain text format.
 - **Comma separated values**
Separates columns separated by commas. Many spreadsheet and database programs allow this format to be imported. It is commonly abbreviated as CSV Format.
 - **Lotus 1-2-3(WK1)**
Select Lotus 1-2-3(WK1) if you are using the file with Lotus 1-2-3.
 - **Microsoft Excel 3.0 (BIFF3)**
Select Microsoft Excel 3.0 (BIFF3) if you are using the file with a version of Microsoft Excel that supports importing of data in BIFF3 format.
 - **Microsoft Excel 4.0 (BIFF4)**
Select Microsoft Excel 4.0 (BIFF4) if you are using the file with a version of Microsoft Excel that supports importing of data in BIFF4 format.
 - **HTML**
Select HTML if you will be using the file with a program that supports HTML formatted files. HTML files are typically displayed using Web browser programs such as Microsoft Internet Explorer or Netscape Navigator.
- 3. Select **Overwrite if file exists** if you want to create a new file each time this query is run.
- 4. Select **Append to file if file exists** if you want to append the results of the SQL query to an existing file each time the SQL query is run. Append to file is only valid for ASCII text and CSV file formats

SQL

The primary use of this tab is to allow you to run the generated SQL statement. You can also:

- Review or edit the generated SQL statement.

- Copy the generated SQL statement to the clipboard. Once copied, the contents of the clipboard can be pasted into any other application that accepts textual data from the clipboard. This is useful if you have another application that will execute a SQL query, but does not provide for easy generation or testing of a SQL query.
- Save the SQL statement for reuse at a later time. This statement is available to you each time you log on to the Database On-Demand applet. You can use this to save common SQL statements that you run multiple times. Queries for getting monthly reports of sales or generating lists of customers who made purchases in the last six months are examples of queries that are good candidates for saving.

Results

Click the Results tab to see query results directed to the display.

Query results appear on this tab after you click Run on the SQL tab or in the Database On-Demand Access window. Each row is represented as a row in the table.

You can change the sort order of any column by clicking on the column header in the table. Clicking again restores the table to the previous ascending or descending order. You may also change the displayed width of any column by dragging the column margin to the right to increase the size or to the left to decrease the size.



Sorting by clicking on the column header is available only in Java 1 browsers without a Java 2 plug-in.

Insert

This tab displays only if you select an Insert SQL statement type on the Tables tab. Insert allows you to insert a new row in your database.

When you finish with the Insert tab, click Next.

The Insert column information is as follows:

1. Column 1 indicates the name of the column in the database row. This can be something generic such as FIELD1 or FIELD2 or it can have a descriptive meaning such as NAME or AGE.
2. Column 2 indicates the type of data that exists in this column in the database. For example, CHAR(4) indicates that up to four characters can be placed in this column.
3. Column 3 is prefaced with an equal sign (=). This column is used to enter the data you want to update in your database column when you create this new row. For example, if your database contains automobile parts, and there is a field called PART# with a type of DOUBLE(8), you would type **10345** to represent a new part number for a steering wheel.

Update

This tab displays only if you select an Update SQL statement type on the Tables tab. Update allows you to modify data in an existing database row.

When you finish with the Update tab, click Next.

The Update column information is as follows:

- Column 1 indicates the name of the column in the database row. This can be something generic such as FIELD1 or FIELD2, or it can have a descriptive meaning such as NAME or AGE.
- Column 2 indicates the type of data that exists in this column in your database. For example, CHAR(4) indicates that up to four characters can be placed in this column.
- Column 3 is prefaced with an equal sign (=). This column is used to enter the data you want to update in your database column when you create this new row. For example, if your database contains automobile parts, and there is a steering wheel part number listed incorrectly as 01234 instead of 10345 in a field called PART#, you would type **10345** on the PART# line containing in the first column.

Delete

This tab displays only if you select a Delete SQL statement type on the Tables tab. Delete allows you to delete records from an existing database table. You can also specify a condition which selects records for the Delete statement to act upon.

When you finish with the Delete tab, click Next.

Database On-Demand File Upload



Database On-Demand provides an interface for uploading files from a client to a host database. The Database On-Demand File Upload feature is entirely different than the iSeries File Upload feature. The advantages of the File Upload feature include:

- Manipulates database data specifically
- Provides for different File Upload statement types
- Uploads [numerous file formats](#)
- Connects to any database using a JDBC driver

The File Upload feature also differs from the Database On-Demand SQL Wizard in that the wizard allows you to work with records in a host database, while File Upload allows you to work with entire files in a host database.

A set of tabs guides you through the process of building and executing a valid File Upload statement. The tabs include:

- [Logon](#)
- [Tables](#)
- [Key Columns](#)
- [File](#)

Logon

Click the Logon tab to connect to the target database. All fields are required.

- **Database URL**

Type the URL for the database you want to work with. Consult your JDBC driver documentation for the format of the database URL. For example, the iSeries Toolbox for Java JDBC driver requires:

```
jdbc:as400://iSeriesname
```

where *iSeriesname* is the fully-qualified network name of the database host.

To use a [proxy server](#) when connecting to the iSeries database, include the proxy server name and port number:

```
jdbc:as400://iSeriesname;proxy server=HODServerName:proxyServerPort
```

- **Userid/Password**

Type your user ID and password for the specified database.

- **Driver description**

Select the JDBC driver used to communicate with the specified database.

- **Class name**

This field contains the class name of the driver associated with the descriptive name in the Driver field.

Enter the required information and Click Connect to open a connection to the host database.

Notes:

- If 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 so that it is not a dll file type and restart your browser. This file is located in the \program files\netscape\communicator\program\java\bin\ directory.
- If you see this message when logging on: Please reset the environment variable CLASSPATH to NULL. you must stop your browser, reset the CLASSPATH to NULL and restart your browser. Check the documentation on your operating system for information regarding how to reset environment variables.
- On Netscape 4.x, you cannot connect to a V5R1 iSeries host that has long password support enabled. The Netscape

4.x JVM does not implement the APIs required to encrypt long passwords. You can use a different browser or install the Netscape 4.x Java 2 plug-in.

After connecting, the connect button is replaced by a Disconnect button, which allows you to disconnect from the database. Also, the following set of tabs are added to the Logon tab:

Tables

Click the Tables tab to specify the tables you want to access in your File Upload statement, and the type of File Upload statement that you will generate.

1. Select the File Upload statement type you want to use. Valid statement types include:

- **Create**

Allows you to create a new table in the host database, using the field descriptions from the existing reference table or a saved SQL statement, and append the data read from the selected file to the new table.

- **Replace**

Allows you to overwrite the contents of the existing host table with data read from the client file.

- **Append**

Allows you to append the data read from the client file to the existing host table.

- **Update**

Allows you to update the existing host table, using specified key columns, with data read from the client file. For example, you could:

1. Use the Database On-Demand SQL Wizard to select which records to download from an existing database table, and save the data to one of the [supported file types](#)

2. Manipulate the data with any program that supports the file type in which you saved the data

3. Upload the entire file to the host database table, instead of updating the records individually with the SQL Wizard

2. If you are creating a table, type a name for the new table, and select whether to use the field descriptions from a reference table, or from a saved SQL statement. Choose either the table or the saved SQL statement you want to access from the list. If you are making changes to a table, choose Replace, Append or Update and select the table the data is replacing, appending to or updating.

3. Click Next.

Click View schema(s) to add tables from additional schemas. A schema is similar to a database or library. For iSeries schemas, the defaults are what is in the default library list for the user profile.

Click Refresh to update the list of tables that are displayed. New tables that were added to the schema are displayed in the Table list; deleted tables are removed. Refresh does not reset any selections that have been made.

When you finish with the Tables tab, click Next.

Key Columns

This tab displays only if you select the File Upload type "Update" on the Tables tab. The available columns window contains the list of the defined columns in the host database table that you can use to uniquely identify the records you want to update.

1. Select one or more columns from the Available columns list.

- Click Select all to select all columns in the list.

- Click Remove all to remove all columns in the list.

2. Use the Add<< and >>Remove buttons to move column names from one list to another.

If the database table you selected already has key columns defined, the key fields are automatically selected from the available columns window and placed in the selected columns window.



You must select the correct columns that uniquely identify the records you want to update, or the update operation results in inconsistent data.

When you finish with the Key Columns tab, click Next.

File

Click the File tab to specify the name of the file to upload. The file type is automatically selected if the file extension is recognized. File Upload supports the following file types:

txt (ASCII)	Plain text format
csv	Columns (fields separated by commas)
wk1	Lotus 1-2-3 format
xls (BIFF3)	Microsoft Excel 3.0 format
xls (BIFF4)	Microsoft Excel 4.0 format



Database On-Demand File Upload cannot support the latest Lotus 1-2-3 or Excel file formats because of the layout and the native methods needed read these files types.

You can save the File Upload statement you have created or updated by clicking Save Statement.

You can upload your file by clicking Run Statement.

Database On-Demand overview



Database On-Demand is a Java applet that performs SQL requests through a JDBC driver. Some Database On-Demand features are:

- A wizard-like interface to aid in constructing SQL or File Upload statements.
- Executable SQL statements, and results that can either be displayed on screen or saved to a file in various formats. Supported formats are:
 - ASCII text
 - Comma-separated values (CSV)
 - Lotus 1-2-3 (WK1)
 - Microsoft Excel 3.0 and 4.0 (BIFF3 and BIFF4)
 - HTML
- Executable File Upload statements that upload data read from client files to the host database. Supported file formats are:
 - ASCII text
 - Comma-separated values (CSV)
 - Lotus 1-2-3 (WK1)
 - Microsoft Excel 3.0 and 4.0 (BIFF3 and BIFF4)
- Statements can be saved for later use. These statements can then be distributed to other Host On-Demand users or groups of users by the administrator.
- The administrator can control Database On-Demand behavior and configuration for a user or a group of users.
- Configuration, administration and data are stored and managed on the server. The administrator does not need to install or configure at a user's workstation.
- The iSeries JDBC driver is shipped and packaged with Database On-Demand. Other user-installed JDBC drivers can also be used.

If you use a [proxy server](#) to connect to an iSeries and you use the Download client, you can decrease the download time when loading the Database On-Demand applet. To do that, edit the CommonJars.js file and replace hoddba.jar with hodpxdba.jar.

This smaller jar file contains only the classes needed for running Database On-Demand when connecting through a proxy server.

Example uses of Database On-Demand

Dynamic queries

Database On-Demand can be used as a dynamic query tool. Without knowing SQL, you can use the SQL statement builder to create an SQL statement or to modify an existing SQL statement. The statement can then be executed or saved for later use.

Saved SQL and File Upload statements

Saved SQL and File Upload statements can be distributed to a user or a group of users. You can simply select the saved SQL or File Upload statement you want to run, then click Run to view the results.

File download

Query results can be saved in many file formats and later imported into your personal productivity program, such as a spread sheet or word processor.

File Upload

Files created from many different formats can be loaded into a host database.

Web page publishing

Database On-Demand supports the writing of query results in HTML using an HTML template file. A template is an HTML document that contains special tags indicating where the query results should be imbedded. The resulting Web page contains everything in the template file, including the query results in the specified location.

Security

Applets running under browsers have limited access to system resources, such as local file access and network access. Database On-Demand requests special permissions from the browser to perform these operations. Browsers display a window asking you to grant or deny these requests. If you deny the request, the applet is not granted the privilege, and the operation fails. Therefore, you have control over what the applet can do from your system.

Using other JDBC drivers

Other JDBC drivers can be used with Database On-Demand; however, due to some browser security restrictions, these conditions apply:

- JDBC drivers that access data locally will not work with Database On-Demand.
- Network JDBC drivers work with Database On-Demand only if the database resides on the same server as the Web server serving the Database On-Demand Web page and applet.

Related topics

- [Configure database options](#)
- [Administer saved SQL statements or File Upload statements](#)

Setting Database On-Demand options for users

Click Database On-Demand Options to customize the behavior of Database On-Demand for individual users. Some of the options define how SQL statements are created, and some of the options define default values.

User options are grouped into the following categories:

- [General](#)
- [Tables](#)
- [Drivers](#)
- [Logon](#)
- [Bidirectional options](#)

An administrator can restrict end-users from modifying options. In this case, end-users do not see the window that includes the restricted option set.

General

- **SQL query timeout**
Select the number of seconds that the driver will wait for a SQL statement to execute. Select a value of 0 to specify no wait limit.
- **Start Trace Facility**
Trace is used to assist in problem determination.

Some host systems use schemas to separate databases or files into groups. For example, you may have separate employee database files (referred to as tables) for each department. These files might be named dept1.employee, dept2.employee, dept3.employee. If you select Use Schema, these tables are displayed with the schema names dept1, dept2, dept3 as part of the table name. If you do not select Use Schema, then only the employee portion of the table name is displayed, preventing the ability to distinguish between multiple tables with the same name.

The value for the SQL query timeout ranges from 0 to 3600 seconds (1 hour). If you experience timeouts due to slow communications networks or slow hosts, you may want to increase the value of this parameter. Specify 0 for no timeout.

Tables

Click this tab to customize the type of table from which you will select when constructing your SQL statement. Select the box next to the table type(s) that you want to display.

JDBC drivers support the ability to limit the table types returned from the database. You can specify which table types should be included.

You can choose to show all table types, or you can specify one or more of the following table types:

- Table
- View
- System table
- Alias

- Synonym
- Global temporary
- Local temporary

Drivers

Click the Drivers tab to register JDBC drivers other than the one provided as part of this program package. You can also remove a driver which has previously been registered.

To register a new driver:

1. Type a description in the Driver description field. This field allows you to associate a descriptive phrase with a specific driver. For example, **iSeries JDBC Driver** or **My favorite Java Database Driver**.
2. Type the class name for the driver you want to associate with the descriptive phrase in the Class name field. Make sure that your class name exactly matches the class name of the driver, including upper and lower case characters.
3. Click Register Driver. The registered driver and description appears in the Registered Drivers section of the window. This indicates it has been registered or will be registered when you click OK.

To remove a previously registered driver:

1. Select the description of the driver you want to remove from the Registered Drivers section.
2. Click Remove.

Logon

Click the Logon tab to set default logon values for the database URL, user ID, and driver to be used when creating new SQL statements. You can also set a default value for the password.

- **Database Name**
Type the URL of the database you want to use. The JDBC driver specifies the proper format of this URL.
- **User ID**
Type the user ID that is used to access the specified database.
- **Driver description**
Select the JDBC driver the SQL commands will use to communicate with the host. The descriptive name of the driver as defined on the Drivers tab, not the actual class name, displays in this field.
- **Save password**
Select this option to use a default password.
- **Password**
Type the password for the user ID. If you selected Save password, the password is saved for future use.

Bidirectional options

Click the BIDI Options tab to set the bidirectional values used at the File Upload statement or the SQL Wizard statement. The BIDI Options tab is visible if your system is configured for Arabic or Hebrew.

- **PC-File Type**

This option specifies whether the PC file you transfer is saved in Logical or Visual format. The default is Logical.

- **PC-File Orientation**

This option specifies whether the PC file you transfer is saved in left-to-right or right-to-left format. The default is Left-to-Right.

Related topics

- [Database On-Demand overview](#)
- [Database On-Demand SQL statements](#)
- [Database On-Demand File Upload Statements](#)



Configuring database options



To configure the database options for a group or user:

1. Click Users/Group in the Host On-Demand Administration window.
2. Right-click the group or user and click Database > Options.

You can configure database options to specify the behavior of Database On-Demand for a specific user or group of users. Some of the options allow or restrict certain functions; other options set default values.

When options are modified for a selected group, all users in that group inherit those settings. 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 group1 and group1 allows deleting SQL statements, and the user is a member of group2 but group2 does not allow deleting SQL statements, the user is allowed to delete SQL statements.

- **User override**

When options are modified for a selected user by either the user or an administrator, 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 group1 which allows edit SQL statements, and group2 which does not allow edit SQL statements, and the user level options do not allow edit SQL statements. The user cannot edit SQL statements, even though group1 allows it.

The table below details how user authority for options is granted.

Allow creating new SQL/Upload statements	Most permissive
Allow save SQL/FileUpload statements	Most permissive
Allow deleting SQL/File Upload statements	Most permissive
Allow manual editing of SQL statements	Most permissive, User override
SQL query timeout	Most permissive (longest wait), User override
Show all table types	Most permissive, User override
Show table	Most permissive, User override
Show view	Most permissive, User override
Show system table	Most permissive, User override
Show alias	Most permissive, User override
Show synonym	Most permissive, User override
Show global temporary	Most permissive, User override
Show local temporary	Most permissive, User override
Allow SQL statement - select	Most permissive
Allow SQL statement - select unique	Most permissive
Allow SQL statement - insert	Most permissive
Allow SQL statement - update	Most permissive
Allow SQL statement - delete	Most permissive
Allow File Upload statement - create	Most permissive
Allow File Upload statement - append	Most permissive
Allow File Upload statement - replace	Most permissive
Allow File Upload statement - update	Most permissive

Allow user to configure Database On-Demand options	Most permissive
Allow user to configure general options	Most permissive
Allow user to configure tables options	Most permissive
Allow user to configure BIDI options	Most permissive
Allow user to register JDBC drivers	Most permissive
Allow user to configure default logon properties	Most permissive

Individual options are grouped into the following categories:

- [General](#)
- [Statements](#)
- [Tables](#)
- [Drivers](#)
- [User Options](#)

General

- **Allow creating SQL or File Upload Statements**
Allows you to create new SQL or File Upload statements.
- **Allow saving SQL or File Upload Statements**
Allows you to save SQL or File Upload statements that you create or modify. This option is valid only if Allow creating SQL Statements or File Upload statements is selected.
- **Allow deleting SQL or File Upload statements**
Allows you to delete previously saved SQL or File Upload statements. You can delete only your own saved SQL or File Upload statements.
- **Allow manual editing of SQL statements**
Allows you to manually edit the generated SQL statement prior to saving it.
- **SQL query timeout**
Used as a timeout value when executing an SQL statement. Choose a number between 0 and 3600 seconds. Choose 0 for no timeout.

Statements

SQL statements

- **Allow select statements**
Allows you to generate statements that use the SQL select clause
- **Allow select unique statements**
Allows you to generate statements that use the SQL Select Unique clause
- **Allow insert statements**
Allows you to generate statements that use the SQL Insert clause
- **Allow delete statements**
Allows you to generate statements that use the SQL Delete clause
- **Allow update statements**
Allows you to generate statements that use the SQL Update clause

File Upload statements

- **Allow Create statements**
Allows you to generate statements that use the File Upload type create
- **Allow Replace statements**
Allows you to generate statements that use the File Upload type replace
- **Allow Append statements**
Allows you to generate statements that use the File Upload type append
- **Allow Update statements**
Allows you to generate statements that use the File Upload type update

Tables

You can select the table types that you want to include.

- **Show All table types**
Shows all defined table types
- **Table**
Show tables
- **View**
Shows views
- **System table**
Shows system tables
- **Alias**
Shows aliases
- **Synonym**
Shows synonyms
- **Global temporary**
Shows global temporary tables
- **Local temporary**
Shows local temporary tables

Drivers

The Drivers tab allows you to register JDBC drivers not provided as part of this program package. You can also remove previously-registered drivers.

User Options

The User Options tab is used to restrict a user's ability to modify certain options. An administrator can grant a user the ability to modify all options, or the ability to modify only selected option groups.

- **Allow user to configure Database On-Demand options**
Allows modification of ALL options.
- **Allow user to configure general options**
Allows modification of the General options.

- **Allow user to configure tables options**
Allows modification of the Tables options.
- **Allow user to register JDBC drivers**
Allows modification of the registered JDBC drivers.
- **Allow user to configure default logon properties**
Allows modification of the default logon properties.
- **Allow user to configure BiDi options**
Allows modification of the BiDi options.

Related topics

- [Database On-Demand Overview](#)



Database statements



Click Statements to manage SQL or File Upload statements previously saved by a group or user. An administrator can copy a statement to another group or user, rename a statement, or delete a statement.

To administer saved SQL or File Upload statements for a group or user:

1. Click Users/Group in the Host On-Demand Administration window.
2. Right-click the group or user and click Database > Statements.

All saved queries for the selected group or user display. If there are no saved queries, an informational message appears.

The administrator can now:

- [Copy a statement](#)
- [Rename a statement](#)
- [Delete a statement](#)

Copy a statement

An administrator can copy saved SQL or File Upload statements from a user or group to another user or group.

When a saved statement is copied to a group, all members of the group have access to the saved statement. Users can run or open the saved statement, if allowed. Users can also save changes to the modified query; however, the changes are saved only to the user's copy of the saved statement, not to the statement saved at the group level.

To copy a saved SQL or File Upload statement:

1. From the Administer Statements tab, select the statement you want to copy.
2. From the Groups and Users tab, select the destination group or user.
3. Click Copy to >>.
4. Modify the Statement Name, if desired.
5. Click OK.

Rename a statement

An Administrator can rename a saved SQL or File Upload statement. After a statement is renamed, the original statement name is no longer valid.

To rename a saved SQL or File Upload statement:

1. From the Administer Statements window, select the statement you want to rename.
2. Click Rename.
3. Modify the statement name.
4. Click OK.

Delete a statement

An administrator can delete a saved SQL or File Upload statement. After a statement is deleted, the original statement is no longer accessible. The delete action is final.

To delete a saved SQL or File Upload statement:

1. From the Administer Statements window, select the statement you want to delete.
2. Click Delete.
3. Click Yes to confirm the delete operation.

Related topics

- [Database On-Demand Overview](#)
- [Database On-Demand SQL statements](#)
- [Database On-Demand File Upload statements](#)



Understanding directories

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.



Migrating to LDAP has [significant implications](#) for your group and user configuration information. Make sure you understand these implications before you migrate.

Additional general information about LDAP and the IBM SecureWay Directory can be found at the [IBM SecureWay Directory Website](#). The IBM redbook *Understanding LDAP*, which can be downloaded from that page, is especially helpful.

Directory

A directory is a specialized database that stores information about objects and their relationships to each other.

For example, in a directory of users, each object might be a person with a user ID and password. These objects may also have application-specific information associated with them, such as group memberships, keyboard mappings, macro definitions, and session parameters.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an open standard that provides an extendable architecture for storage and management of directory information. Widely accepted and fast-growing, LDAP has become the *de facto* industry standard for accessing directory information over a TCP/IP network.

Distinguished Name

A distinguished name (DN) consists of one or more relative distinguished names (RDNs) arranged in a hierarchical, tree-like structure to uniquely identify a single directory entry. This tree-like structure is organized from more general to more specific, going from the root of the tree to the leaves, and is called a directory information tree (DIT). The arrangement of the RDNs in the DN reflects this tree-like structure. From left to right, the RDNs are arranged from most specific to least specific and are separated by commas.

For example, `cn=Chris Smith,o=IBM,c=US` is a DN that consists of three RDNs that uniquely identify Chris Smith. `c=US` is an RDN that branches from the root of the DIT, `o=IBM` is an RDN that branches from RDN `c=US`, and `cn=Chris Smith` is an RDN that branches from RDN `o=IBM`.

Each RDN is derived from the attributes of the directory entry. In the simple and common case, an RDN consists of an attribute value pair that has the form *attribute name = value*. For more information, refer to the documentation for the LDAP directory service for your environment.

Related topics

- [Setting up and using LDAP](#)
- [Specifying the LDAP directory information](#)
- [Migrating to an LDAP directory](#)



Setting up and using LDAP



Before you can use LDAP, you must:

1. [Select an LDAP directory](#)
2. [Install the Host On-Demand schema extensions](#)
3. [Create a suffix to store Host On-Demand configuration information](#)
4. [Create an administrator distinguished name and password](#)

To set up and use LDAP:

1. Click Directory Service in the Administration window.
2. Check the Use Directory Service (LDAP) checkbox.
3. [Specify the LDAP Directory Information.](#)
4. Optionally, [select Migrate Configuration to Directory Service.](#)
5. Click Apply.

After you click Apply, the Host On-Demand server attempts to connect to the LDAP server using the information you provided. If communication to the LDAP server cannot be established or if the LDAP administrator does not have the required privileges within the specified Host On-Demand suffix, the process fails. An error message then appears that describes the problem. After correcting the problem, click Apply again. A status message appears at the bottom of the Directory tab when the new directory settings have been successfully applied.

Limitations

- Host On-Demand requires JDK1.1.6 or later when using LDAP on Host On-Demand servers for non-Windows platforms.
- Enabling LDAP causes the Host On-Demand service manager to stop. This is due to Just In-Time (JIT) compiler problems in JDK1.1.8 when running on AIX 4.3.3. Disable the JIT by replacing any statement that uses the java command with `jre -nojit`.
- You cannot change your user password with LDAP enabled if you are running Host On-Demand on a Linux client and connecting to a Linux server.

Migration

If you select **Migrate Configuration to Directory Service**, migration will be attempted when you click Apply. A dialog box with a progress indicator will appear while migration is being performed. To cancel migration, click Cancel; migration will stop after it finishes processing the current user or group.



Migrating to LDAP has [significant implications](#) for your group and user configuration information. Make sure you understand these implications before you migrate.

Related topics

- [Specifying the LDAP directory information](#)
- [Implications of migrating to LDAP](#)
- [Understanding directories](#)



Specifying the LDAP directory information

This task is part of [setting up and using 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=Chris Smith,o=IBM,c=US`).

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, `cn=HOD,o=IBM,c=US`).

Directory schema

An LDAP directory server is shipped with a predefined schema. The object classes that a directory server can store and the attributes that these objects can contain are defined by its schema. The schema defines which object classes can be created and where they may be located within the DIT. In addition, the schema defines the syntax of an object's attributes and specifies which attributes are required and which are optional.

Related topics

- [Migrating to an LDAP directory](#)
- [Implications of migrating to LDAP](#)
- [Understanding directories](#)



Migrating to an LDAP directory

This task is part of [setting up and using LDAP](#).



Migrating to LDAP has [significant implications](#) for your group and user configuration information. Make sure you understand these implications before you migrate.

To migrate users and groups to an LDAP directory, click Directory Service in the Administration window and click **Migrate Configuration to Directory Service**.

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** check box is automatically cleared. Simply select it and click Apply, and the migration process will begin again.

Notes:

- Migrating on an iSeries can be a lengthy process, sometimes taking up to 40 minutes to complete. Host On-Demand will only show that the system is busy. Please be patient.
- Defining a large number of users can significantly slow down Host On-Demand server. It is recommended that you limit the maximum number of users in any one group to be in the range of 50 to 100.
- If the administrator log on fails when enabling LDAP using a Netscape LDAP server, disable UID uniqueness, restart the HOD Service Manager and re-enable LDAP.

To disable UID uniqueness in Netscape LDAP Server:

1. Go to the Configuration tab and expand the plugins item. The last item should be UID uniqueness.
2. Select UID uniqueness and you will see a checkbox labeled "Enabled".
3. Clear the UID uniqueness checkbox.
4. Restart the LDAP server.

Related topics

- [Specifying the LDAP directory information](#)
- [Understanding directories](#)



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 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 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.

Related topics:

- [Setting up and using LDAP](#)
- [Specifying the LDAP directory information](#)
- [Migrating to an LDAP directory](#)
- [Understanding directories](#)

Sources for troubleshooting information

This page provides information that will assist you in determining what is causing the problem you are experiencing and how to fix the problem, before calling IBM for assistance. You can search the [online documentation](#) provided and the [documentation on the Web](#) for assistance; and then you can take the recommended course of action or apply the recommended [service updates](#).

Online documentation

IBM provides the following online documentation to assist you in using Host On-Demand:

- The [Readme](#), in HTML format, is installed with Host On-Demand. The Readme contains information that became available too late for inclusion in the publications or the Help.
 - On Windows platforms you can access the Readme by clicking Start > Programs > Host On-Demand > InfoCenter > Readme.
 - On S/390, AIX, Linux, HP-UX and Solaris, you can access the Readme in the `hostondemand/hod/en/doc/readme` directory as `readme.html`.
 - From the Host On-Demand CD, you can access the Readme as `readme.html` from the `\readme\xx` directory, where `xx` is the two-letter language suffix for your country or region. See the [Planning, Installing, and Configuring Host On-Demand guide](#) for a list of supported languages and their corresponding language suffixes. For example, the language suffix for English is `en`, so the directory on the CD is `readme\en`.

The Readme is provided with the base version of the product. Each time a service update is provided, such as a Program Temporary Fix (PTF) or Corrective Service Disk (CSD), the Readme is updated with additional information. These updates allow you to see all the updated information from the base product version to the latest service update in one file.

- The [online help](#) is installed with Host On-Demand. The online help defines the fields and panels on the user interface and their associated values. It also documents the steps necessary to perform various tasks and provides some conceptual information about Host On-Demand. Online help is available in HTML format.
- The [Planning, Installing, and Configuring Host On-Demand](#) guide is installed with Host On-Demand. It provides the information to install Host On-Demand and configure it so that you can use sessions. This guide is available in HTML and PDF format.
- The [Host Printing Reference](#) is installed with Host On-Demand. It explains how to configure 3270 and 5250 host printing. This guide is available in HTML format.

If you install the Host Access Toolkit, you also receive the following documentation:

- The *Host Access Toolkit Getting Started* guide, which provides the information needed to install the Host Access Toolkit. This guide is available in HTML and PDF format.
- *Host Access Beans for Java*, which describes how to use the Host Access Beans for Java to provide emulator functions as a set of JavaBeans. Documentation for this API is supplied in HTML format.
- *Host Access Class Library* (HACL), which explains how to use the core set of Java classes and methods that allow the development of platform independent applications that can access host information at the data stream level. Documentation for this API is supplied in HTML format.
- *Host On-Demand J2EE Connector*, which explains how to use the Host On-Demand J2EE Connector, a Java programming interface that conforms to the J2EE Connector Specification version 1.0 from Sun Microsystems and the Common Client Interface (CCI) infrastructure. Documentation for this API is supplied in HTML format.

Troubleshooting checklist

[Troubleshooting Host On-Demand](#) contains resources for finding troubleshooting information on the Web and a checklist for identifying common Host On-Demand problems.

Problem determination aids

[Problem determination aids](#) explains the Host On-Demand tools that are available to assist you in identifying and fixing problems.

Web documentation

The WebSphere Host On-Demand page is the starting point for Host On-Demand user assistance on the Web. The URL is:

<http://www-4.ibm.com/software/webservers/hostondemand/>

For technical information, you can follow these links:

The [Host On-Demand Support page](#) provides links to technical information such as Host On-Demand News, Service Updates, Hints and Tips, and the Library. The URL is:

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

Hints and Tips are brief instructions that explain technical issues discovered too late to be included in the documentation. Topics include installation, configuration, troubleshooting, and usage issues. Hints and Tips are dynamic; they are updated every few weeks, while the Readme is only updated when a CSD is made available.

The [IBM Support page](#) provides access to technical information for additional IBM Products. The URL is:

<http://www.ibm.com/support>

[IBM WebSphere Software Support Bulliten](#) is a e-mail monthly newsletter that highlights the latest code fixes, support information, and hot tips about IBM WebSphere Software products, including Host On-Demand, once you have subscribed to it. The URL is:

<http://www.ibm.com/software/network/support/alert/>

Service updates

You can access the latest service updates from the [Host On-Demand Support page](#). The URL is:

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

To determine the Host On-Demand service level on your system:

1. Start an emulator session.
2. Click Help > About Host On-Demand. The Host On-Demand about window displays.
3. Look at the number on bottom of the About window. The number determines the service level. For example, if you see 5.0.3-B20000814, it means:
 - 5 is version number.
 - 0 is the release number.
 - 3 is the maintenance, or CSD level.

4. Match this information to the Host On-Demand Support page, under Service Updates pages, to determine service level.

To download the latest service updates for Host On-Demand, you will need to register with the [IBM Software Internet Service Delivery](http://www6.software.ibm.com/aim/home.html) site. The URL is: `http://www6.software.ibm.com/aim/home.html`.

This site entitles customers to download service updates directly from the Internet. After registering, you need to add the Service Key to your registration. The Service Key is the 10 digit number on the Service Key Card that is provided with the product. Then you can download the product that matches the key you have entered. You may register multiple keys to the ID you created when you registered.

The Service Key must be treated with the same care given to the base product in terms of Export and Import regulations, since it provides access, through the Web, to code which 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 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.

Need help from IBM?

If you are unable to resolve your problem after reviewing this information, you may [need help from IBM](#). You should collect the suggested information before contacting IBM.

Troubleshooting Host On-Demand

- [Web resources for troubleshooting](#)
- [Troubleshooting checklist](#)
- [Before you call IBM for assistance](#)

Web resources for troubleshooting

Check the Host On-Demand Web pages on the Internet for additional information and help. The following sites provide up-to-date support information on code fixes, newsgroups, and other support:

1. [Sources](#) with the latest troubleshooting information.
2. Host On-Demand [Publications](#)
3. Host On-Demand Support [Web Page](#)
4. IBM WebSphere Software Support [newsletter](#)
5. Latest [service updates](#)

Troubleshooting checklist

Use the following checklist to identify and find solutions for problems that are occurring with your Host On-Demand installation.

1. **Did you receive an error message?**
 - a. Did the message appear on the bottom of the emulator window?
See the [OIA \(Operator Information Area\) help](#).
 - b. Did a pop-up message appear?
See the [error message help](#).
 - c. Did a message from the Host On-Demand Service Manager appear?
See the [Service Manager](#) help.
 - d. Did a Java event occur?
See the [Java Console or Java log](#) for messages about Java events.
See [Java Troubleshooting Checklist](#).
2. **Did the problem occur during installation of the Host On-Demand server?**

Check the installation instructions for your platform:

- a. Installing on zSeries, located in the Program Directory. (The most up-to-date version of the Program Directory can be found on the Host On-Demand Web site, <http://www.ibm.com/software/webservers/hostondemand/>.)
- b. [Installing on iSeries](#)
- c. [Installing on Windows platforms](#)
- d. [Installing on AIX](#)
- e. [Installing on the Solaris, HP-UX, and Linux platforms](#)

f. [Installing on OS/2](#)

g. [Installing on Novell NetWare](#)

3. Did the problem occur during installation of the Configuration Servlet?

Check the installation instructions for your platform:

a. [Installing the configuration servlet on the Windows and AIX platforms](#)

b. [Installing the configuration servlet on the iSeries platform](#)

4. Did the problem occur during installation of the Deployment Wizard?

Check the Deployment Wizard installation instructions:

a. [Installing the Deployment Wizard from the Windows CD](#)

b. [Downloading the Deployment Wizard installation image from a Host On-Demand server](#)

5. Did the problem occur only on the zSeries platform?

See [zSeries Troubleshooting Checklist](#).

6. Did the problem occur only on the iSeries platform?

See [iSeries Troubleshooting Checklist](#).

7. Did the problem occur while you were configuring HTML pages with the Deployment Wizard?

See the following:

a. [Using the Deployment Wizard](#) for an overview of how to use the Deployment Wizard.

b. [Deployment Wizard Troubleshooting Checklist](#).

8. Did the problem occur while you were configuring the Redirector?

See the following:

a. [Server trace and message facility](#) for instructions on how to collect information about the Redirector and configuration services.

b. [Redirector Troubleshooting Checklist](#).

9. Did the problem occur while you were configuring TLS or SSL?

Do the following:

a. Review your TLS or SSL configuration and setup. See [Configuring SSL clients](#).

b. See [Security Troubleshooting Checklist](#).

10. Did the problem occur while you were configuring the AS/400 proxy?

See [OS/400 Proxy Server](#).

11. Did the problem occur while you were configuring Host On-Demand users and sessions?

See the following:

a. [Basic Configuration Steps](#) for an overview of Host On-Demand configuration.

b. [Managing users and groups](#) for an overview of how to manage users and groups.

c. [Working with sessions](#) for an overview of how to manage sessions.

12. Did the problem occur while you were setting up dynamically modified session properties (HTML overrides)?

See [Modifying session properties dynamically](#).

13. Did the problem occur while downloading clients?

See [Client Troubleshooting Checklist](#). The following are some known client problems:

- a. The client does not [download](#).
- b. The client downloads [slowly](#).
- c. The client does not [connect](#).
- d. [You receive](#) a LOG0001 message.
- e. A [port](#) is inaccessible.
- f. The [Screen Customizer interface](#) doesn't work with an emulator client.

14. Did the problem occur while using a 3270 or 5250 emulator client?

The following are some known emulator client problems:

- a. The client does not [connect](#).
- b. The [Screen Customizer interface](#) doesn't work with an emulator client.
- c. [classes.zip CLASSPATH entry may cause connection problem](#)

15. Did the problem occur while using FTP?

The following are some known FTP client problems:

- a. The client does not [connect](#)
- b. [classes.zip CLASSPATH entry may cause connection problem](#)

16. Did the problem occur while using Database On-Demand?

The following are some known Database On-Demand client problems:

- a. The client does not [connect](#)
- b. [classes.zip CLASSPATH entry may cause connection problem](#)

17. Did the problem occur when you started or ran the Service Manager?

Do the following:

- a. Check the operating system's message logs or operator consoles.
- b. Check for Service Manager errors posted in NCoDServiceManager.txt
- c. See the [Java Console or Java log](#) for messages about Java events.
- d. Use the [Server trace and message facility](#) to collect information about configuration services.
- e. Use the [Service Manager trace](#) facility to collect trace information about the Service Manager.

18. Did the problem occur while printing?

Do the following:

- a. Check the printer status window of the printer session to view [printer status and messages](#).
- b. See [Printing Troubleshooting Checklist](#).
- c. See the [printer datastream information](#) in the *Host Printing Reference*.
- d. See the [log file for the printer definition table](#).

19. Is the problem related to which browser you are using?

See [Browser Troubleshooting Checklist](#).

20. Does the problem not fall into any of these categories?

Check the [Miscellaneous items](#) for a list of known troubleshooting issues not otherwise covered in this list.

Before you call IBM for assistance

Use the checklist

Use this [checklist](#) to gather information about your Host On-Demand problem before calling IBM for assistance. This will make it easier for IBM to help you.

Gather trace information

See the following help topics for instructions on gathering trace information to help your IBM service representative diagnose problems with Host On-Demand:

1. [Tracing on the client](#) for instructions on how to use the client trace facility.
2. [Tracing on the server](#) for instructions on how to use the server trace facility.
3. [Client trace and message facility](#) for trace information about host sessions.
4. [The TraceOptions HTML Parameter](#) for trace information about host sessions using the TraceOptions parameter in the client HTML file.
5. [Java Console \(Netscape\) or Java log \(Internet Explorer\)](#) for information about Java events.
6. [Transport trace](#) for trace information about Telnet TCP/IP Emulator data flow between the client and Telnet server.
7. [IPMonitor](#), a Java utility you can use to collect trace information containing the session data flowing between a client and a host.
8. [Server trace and message facility](#) for collecting trace information about the Redirector and configuration services.
9. [Service Manager trace](#) for collecting trace information about the Service Manager.

Problem determination aids

The following traces and logs can help you find and resolve problems:

- [Server trace and message facility](#) collects information about the Redirector and configuration services.
- [Messages](#), which list the Host On-Demand error messages.
- [Client trace and message facility](#) collects information about host sessions.
- [Java Console \(Netscape\) or Java log](#) (Internet Explorer) collects information about Java events.
- [Printer Definition Table Compiler log](#) collects information when you create a PDT.
- [Operator Information Area](#) (OIA) in the session window displays session status and messages.
- [Printer Status window](#) of a printer session displays printer status and messages.
- Host On-Demand [Service Manager messages](#) provide information regarding the Service Manager.
- [Transport trace](#), which captures the Telnet TCP/IP Emulator data flow between the client and Telnet server.
- [IPMonitor](#), a Java utility you can use to collect trace information containing the session data flowing between a client and a host.
- [Information Bundler](#) gathers diagnostic information from a Host On-Demand server installation.
- [Service Manager trace](#) collects information about the Service Manager.
- [Tracing the client download](#) gathers diagnostic information about client downloads.
- [Web pages for more help](#)

Server trace and message facility

The server trace and message facility is always installed and is available through the Services page of the Administration window. From Services, you can start and stop Redirector tracing and view the server's Trace/Message Console, which lets you see the trace and message information on the screen. The information is also saved in NCoDServices.RAS.txt in the private directory. You can look at this file with any ascii text editor. See [Host On-Demand services](#) for more information.

Client trace and message facility

The client trace and message facility is available only if on clients that include the problem-determination functions. These clients include:

- Cached client (HODCached.html)
- Problem Determination client (HODDebug.html)
- Database client (HODDatabase.html)
- Administration client cached with problem determination (HODAdminCachedDebug.html)
- New user client cached with problem determination (NewUserCachedDebug.html)

From the Actions menu in a host-session window, you can choose to view the log messages, which opens the Message Console, or to open the Trace Facility window. You can also do the latter by clicking the Trace button on the toolbar. For Database On-Demand, you can set up tracing by clicking Options > Trace > Start Trace Facility.

The information in the Message Console is saved in the same file as the trace information, but you can also copy it to the clipboard and save it in a text file. You may be asked to do this by service personnel.

When you start the Trace Facility, you have to make several choices about which function or component you will trace

and about the trace level, which determines the amount of data that will be collected. You can also decide whether to save the data to the Java Console or Log, and to the server or to the local disk. In general, an IBM service person will tell you what the settings should be.

As an administrator, you will either have to tell a user how to start a problem-determination client and what choices to make, or load the client yourself and try to reproduce the problem.

We recommend you save the file locally on the client, in case you need to send the file to a system administrator or IBM support. Also, if you save the file locally, you can choose the directory in which to save the file.

For more information about using the message and trace facilities, refer to:

- [Configuring the TraceOptions HTML parameter](#)
- [The TraceOptions HTML parameter](#)
- [IP Monitor](#)
- [Viewing a User's Trace](#)
- [Tracing on the Server](#)
- [Tracing on the Client](#)
- [Log and Trace Messages Format](#)
- [Setting Trace Levels](#)
- [Changing the trace settings \(client\)](#)


The Java console or log

The [Java Console](#) or Log collects information about Java events, but you can also choose to have Host On-Demand messages and trace data saved here. You can turn on the [Java Console](#) for both Netscape and Internet Explorer. You can also view the Microsoft Javalog.txt in the Java directory (winnt\java) on Windows.

Printer Definition Table Compiler log

The Printer Definition Table Compiler log (pdtc.log) collects progress and error information each time you create a PDT. The error information is intended to help you make corrections to the PDF that you have customized.

Operator Information Area (OIA)

The Operator Information Area (OIA) is normally visible at the bottom of a session window, though it can be turned off when a session is configured. The OIA contains several items of information that indicate the status of the session and of its connection. In Host On-Demand 7.0, a  displays when a session is encrypted. Referring to the [OIA Help](#) will often enable you to resolve a problem.

Printer status window

The Printer Status window of a printer session is the equivalent of the session window of a display session. It provides a graphical display of the connections between the host system or server, the session and the printer, and displays various error messages. It is fully described in the [Help](#). There is more specific information about resolving printer-session problems in the [Troubleshooting appendix](#) of the Host Printing Reference.

Service Manager messages

On a client, you might see the message:

```
System problem. Contact your system administrator. Error= -41.
```

On a server, you might see:

```
LOG0001: Host On-Demand cannot be used....
```

These messages indicate one or more of the following:

- The Service Manager is on the other side of a firewall and the browser cannot connect to it. This might be because a port that the Service Manager uses, such as 8989 or 8999, is not open on the firewall.
- A network problem has prevented connection to the Service Manager.
- The Service Manager is not started or is not operational.

Host On-Demand Transport Trace

The Transport Trace captures the Telnet TCP/IP Emulator data flow between the client and Telnet server. Use the problem determination clients to capture the data flow. For example, you can use `HODDebug.html`. You can access the problem determination clients from `HODMain.html`.

1. Start the host session you want to trace, and log on to the host system.
2. Select Assist from the session menu.
3. Select Problem Determination.
4. Select Trace Facility.
5. Click Host Access Class Library in the Function window to highlight it.
6. Click Transport in the Component window to highlight it.
7. Click Level 1 in the Trace Level window to highlight it.
8. Click Settings.
 - Set the file to be saved on the local machine.
 - Click OK.
9. Click Start.
10. End the session. You must return to your Host On-Demand start page, for example, `HOD.html`.
11. Start the session again.
12. Follow the steps to recreate the problem.
13. Click Stop.
14. Click Save. The Save window displays.
15. Select location to save the trace file to, and name the trace file.

IPMonitor

IPMonitor is a Java utility you can use to collect trace information containing the session data flowing between a client and a host. IPMonitor is an intermediary between a client and a host. The client connects to IPMonitor, while IPMonitor connects to the host. IPMonitor then records session data flowing between the client and the host. You can start IPMonitor as a Java application or as a Java applet.

You start and configure IPMonitor differently, whether IPMonitor is running as an application or an applet, and which version and release of Host On-Demand you are running.

IPMonitor for Java on Host On-Demand V6

- [IPMonitor](#)
- [Configuring the IPMonitor HTML parameter](#)
- [IPMonitor v1.0 for Java](#)
- [Using the IPMonitor v1.0 for Java application](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting the IPMonitor v1.0 for Java, normal mode applet from the Run Applet session menu option](#)

Information Bundler

Use the Information Bundler to collect diagnostic information from a Host On-Demand server. The Information Bundler stores copies of the following in a zip file:

- Registry keys (Windows NT, Windows XP, and Windows 2000 systems only)
- Private files
- Security files
- Published HTML files
- Properties files
- JavaScript files
- NSM properties files
- Deployment Wizard files
- Printer Definition files
- DirUtil files
- User-defined font files
- DWUnzip files
- IPMonitor trace files
- Custom groups of files that you configure in the configuration file

User-defined font files will not be present on the Host On-Demand server unless created by the user.

The zip file can then be sent to your IBM Support Center to assist in diagnosing problems.

You can run the Information Bundler through a graphical user interface (on all supported platforms except Novell, OS/400, and z/OS) or through the command line.

- [Running the Information Bundler](#)
- [Information Bundler command line options](#)
- [Information Bundler graphical user interface](#)
- [Adding a custom extension to the Information Bundler](#)

Running the Information Bundler

To run the Information Bundler, do the following:

- On the Windows NT, Windows 2000, and Windows XP platforms, do one of the following:
 - Choose **Start > Programs > IBM Host On-Demand > Administration > Information Bundler**
 - Run the following script:
`install_dir\lib\samples\InfoBundler\InfBnd.cmd`

- On the AIX platform, run the following script at the command line:

```
install_dir/lib/samples/InfBndCommandFiles/InfBnd-AIX
```

- On the Solaris and Linux platforms, run the following script at the command line:

```
install_dir/lib/samples/InfBndCommandFiles/InfBnd-UNIX
```

- On the Novell Netware platform, run the following script at the command line:

```
install_dir/lib/samples/InfBndCommandFiles/InfBnd-Novell.ncf
```

- On the OS/2 platform, run the following script at the command line:

```
install_dir/lib/samples/InfBndCommandFiles/InfBnd-OS2.cmd
```

- On the OS/400 platform, run the following script at the command line:

```
install_dir/lib/samples/InfBndCommandFiles/InfBnd-OS400.sh
```

- On the z/OS platform, run the following script at the command line:

```
install_dir/lib/samples/InfBndCommandFiles/InfBnd-S390
```

In these commands, *install_dir* is the installation directory for the Host On-Demand software.

To see a list of the command-line options, invoke the Information Bundler without any parameters or with the `-?` parameter. For more information, see [Information Bundler command line options](#).

Information Bundler graphical user interface

The Information Bundler graphical user interface (GUI) is available on all supported platforms except Novell, OS/400, and z/OS. To access the GUI, invoke the Information Bundler with the `-gui` parameter.

The Host On-Demand Information Bundler window opens.

1. Specify the desired Host On-Demand publish directory, if it is not the default publish directory.
2. Specify the alternate Host On-Demand publish directory for Deployment Wizard files. This field should be set to the same path as the Directory field in the Deployment Wizard Summary panel. The default path is the Host On-Demand publish directory.
3. Select the types of information to be gathered. If you are gathering IPMonitor trace information, specify the name of the trace file. To do this, select the IPMonitor Trace Files button, which opens a separate dialog. Then, browse to a particular .TLG file or search a directory for .TLG files.
4. Specify the output file.

The default output file is `install_dir\private\hodpd.zip`.

Any existing output file will be overwritten. You will not be prompted first.

If you select to rename the output file, the Information Bundler will not automatically add a .zip extension to the

file.

5. Click OK. The selected files are added to the zip output file.

Information Bundler command-line options

The Information Bundler can be accessed through the command line on all supported Host On-Demand platforms.

To see the command line options, run the Information Bundler from the command line with the `-?` parameter or without any parameters.

For information on running the Information Bundler on all Host On-Demand platforms, see [Running the Information Bundler](#).

In order to specify all the command line parameters that you want to specify, you may need to edit the line of the command script that invokes the Information Bundler. Originally, this line specifies a limited number of symbolic parameters (such as, `%1 %2`, and so on, or `$1 $2`, and so on) instead of actual parameters.

On platforms that support the GUI, if you want to run the Information Bundler with command line options rather than with the GUI, edit the line of the command script that invokes the Information Bundler to remove the `-gui` parameter. Otherwise, the `-gui` parameter will override the command line options.

Adding a custom extension to the Information Bundler

You can add custom extensions to the default Information Bundler configuration file, `infbnd.properties`. You can also specify a different configuration file. The configuration file indicates what types of information can be selected to include in the zip file. You can also add new types of information and specify what files will be gathered when that new type is selected.

To specify a different configuration file, use the `-cfg` parameter, followed by the name of the configuration file that you would like to use. A path name that is not absolute will be searched for, starting in the Host On-Demand installation directory. For more information on command line options, see [Information Bundler command line options](#).

To add a custom extension to the default configuration file, follow these steps:

1. Make a backup copy of the `infbnd.properties` file, which is located in the Host On-Demand publish directory.
2. Choose one of the 32 extension information categories (Extension01 - Extension32), and add the category to the `InfoCategoryList`. The following example shows the default `InfoCategoryList` with *Extension01* added to the end:
`InfoCategoryList: \ HODRegKeys ; \ PrivateDir ; \ SecurityFiles ; \ HTMLFiles1 ; \ PropFiles1 ; \ JavaScriptFiles ; \ NSMPropFiles ; \ DepWizFiles ; \ PrtDefFiles ; \ DirUtilFilesWin32 ; \ DirUtilFilesNonWin32 ; \ UdfFiles ; \ Extension01`
In the above example, be sure to place a `\` character at the end of the line after `UdfFiles`.
3. Modify the sample `Extension01` `InfoCategory` at the end of the `infbnd.properties` file.
4. Modify the sample `WorkItem` elements for `Extension01` at the end of the `infbnd.properties` file.
5. Copy the updated configuration file to the Host On-Demand publish directory.
6. Run the Information Bundler with the updated configuration file.
7. Run the Information Bundler from the console rather than using an icon in order to see if there is an error in the new configuration file. If there is an error, the Information Bundler will write a general error message to the console and will write a description of the specific error into the log file. The log file is named `infbnd.log` and is located in the install directory.

The following are definitions of the elements used in the configuration file:

`InfoCategoryList` and `InfoCategory` names

The `InfoCategoryList` is the top-level element of the configuration file. This element consists of the term `InfoCategoryList`, followed by a list of `InfoCategory` names. Examples of `InfoCategory` names are: `HODRegKeys`, `PrivateDir`, and `SecurityFiles`. Each `InfoCategory` name refers to a group of similarly named data elements (constituting an `InfoCategory`) contained in the configuration file. An `InfoCategory` includes: an `InfoType`, a

DisplayName, a CmdLineOption, a Platform element, a ZipDir, and one or more WorkItems.

InfoType

This element identifies the type of information to be collected. Valid types are FileSet and RegKeySet. The name of this element is formed as follows: InfoCategory name + _InfoType.

DisplayName

This element identifies the message key used by Host On-Demand for the message to be displayed to the user in the Information Bundler Java GUI panel (for example, KEY_IB_EXTENSION_01 causes *Extension01* to be displayed). These messages are defined as follows: KEY_IB_EXTENSION_xx, where xx is the extension number (01-32). The name of this element is formed as follows: InfoCategory name + _DisplayName.

CmdLineOption

This element specifies the text string to be used as a command line option to identify an information category. Examples of this are: sec, for SecurityFiles; ext01, for Extension01. On the command line, the command line parameter must be preceded by a '-' (for example, '-ext01'). The name of this element is formed as follows: InfoCategory name + _CmdLineOption.

Platform

This element specifies the platform types on which the information category is valid. Valid platform types are: AIX (including Linux and Solaris), Win32, OS/400, and MVS. For example, the HODRegKeys category is valid only for the Win32 platform type. When the utility is run, a category that is not valid for the current platform is skipped. The name of this element is formed as follows: InfoCategory name + _Platform.

ZipDir

This optional element specifies a text string to be used as a top-level ZIP entry directory for an Information Category (for example, *test* would cause all ZIP entry paths for the information category to begin with *.\test*). The name of this element is formed as follows: InfoCategory name + _ZipDir. For no ZIP entry directory name, specify *none*.

WorkItemList and WorkItem references

This element specifies a list of one or more sets of information to be collected. The name of this element is formed as follows: InfoCategory name + _WorkItemList (for example, Extension01_WorkItemList). The list must contain one or more WorkItem references. A WorkItem reference has the form: WorkItem_ + numeral (for example, WorkItem_1, WorkItem_2).

WorkItem

This element describes a set of information to be collected. The name of this element is formed as follows: InfoCategory name + _ + WorkItem reference (for example, Extension01_WorkItem_1). When the InfoType is FileSet, the WorkItem contains the following subelements: DirType, DirName, SubdirSearchDepth, Include, and Exclude. When the InfoType is RegKeySet, the WorkItem contains RegKey subelements.

PlatformWI

This subelement can occur within a WorkItem element when the InfoType of the InfoCategory is FileSet. This subelement is optional. For the WorkItem in which it occurs, this subelement narrows the scope of the Platform command which otherwise controls the InfoCategory. For example, the SecurityFiles InfoCategory has SecurityFiles_Platform set to "win32; aix; mvs; os400", indicating that this InfoCategory applies to all 4 platform types. However, Security_Files_WorkItem_1 has a PlatformWI subelement set to "win32, aix, mvs", indicating that this particular work item applies only to the 3 specified platform types.

DirType

This subelement occurs within a WorkItem element when the InfoType of the InfoCategory is FileSet. This subelement describes the relation of the directory to be searched to the system's file structure. Valid types are:

RelativeToInstall

The utility will search in the Host On-Demand install directory for the subdirectory specified in the DirName subelement.

RelativeToPublish

The utility will search in the Host On-Demand publish directory for the subdirectory specified in the DirName subelement.

RelativeToDir

The utility will search in the subdirectory specified in the DirName subelement.

Absolute

The utility will ignore the DirName element and search for the file using the file path specified in the Include subelement.

DirName

This subelement occurs within a WorkItem element when the InfoType is FileSet, and when the DirType is RelativeToInstall, RelativeToPublish, or RelativeToDir. This element specifies the path of the subdirectory to be searched. The value may be any valid path including .. For RelativeToInstall and RelativeToPublish, the DirName should be a relative directory path. For RelativeToDirectory, the DirName should be an absolute directory path.

SubdirSearchDepth

This subelement occurs within a WorkItem element when the InfoType is FileSet. This element specifies how many subdirectories deep the search for Include files should continue from the beginning directory. Valid values are: 0, 1, 2, 3, etc.. . To search all subdirectories, specify *all*. The maximum allowed search depth is determined by the amount of memory available in the Java Virtual Machine.

Include

This subelement occurs within a WorkItem element when the InfoType is FileSet. This subelement specifies a list of one or more files to be collected. The file name after the last file separator may contain the wild card characters '?' (which matches any one character, except '.') and '*' (which matches 0 or more characters, except '.'). When the utility runs, it will attempt to collect all files matching the pattern.

Exclude

This subelement occurs within a WorkItem element when the InfoType is FileSet. This subelement specifies a list of one or more files to be excluded. The file name after the last file separator may contain the wild card characters '?' (which matches any one character, except '.') and '*' (which matches 0 or more characters, except '.'). When the utility runs, it will reject files matching the pattern.

RegKey

This subelement occurs within a WorkItem element when the InfoType is RegKeySet. This subelement defines a Microsoft Windows registry subkey to be read.

Service Manager trace

The Service Manager trace facility is available through the Services page of the Administration window. Use this facility to gather troubleshooting information about the Service Manager. From the Services page, click Service Manager Trace to start and stop tracing and set the trace level. See [Host On-Demand services](#) for more information.

Tracing the client download

To gather trace information about client downloads, update the HTML file that downloads the Host On-Demand client by editing the HTML with the Deployment Wizard. Check Debug Cached Client and add an additional parameter of DebugCode with a value of 65535.

IBM will need a detailed Web server trace showing the files being downloaded and any error message logs produced by this Web server. For an HTTP webserver, the trace is called a VV trace (very verbose), or LOGLEVEL of debug.

Web pages for more help

The following site provides up-to-date support information. Find information about code fixes, newsgroups, and other support:

<http://www.ibm.com/software/webservers/hostondemand/support>

Before you call IBM



If you have followed the procedures outlined previously for the type of web browser you are using and have determined that you need IBM assistance to solve your problem. The following is a list of the information that the IBM Support Center may need to help diagnose your problem. You can print a copy of this list, and then fill in the blanks, before contacting IBM for service.

Description of the problem and the environment

1. Problem Summary:

2. Host On-Demand version, release, and CSD level_____.

To determine the Host On-Demand version, release, and CSD level, click Help > About Host On-Demand from the session window. The About window displays. Look at the number on bottom of the About window. The number, in 0.0.0-B00000000, determines the version, release and CSD level. For example, you may see 6.0.3-B20000814, where:

- 6 is version number.
- 0 is the release number.
- 3 is the maintenance, or CSD level.

3. If you are using the Host On-Demand Administration client, is the client on the same machine as the Host On-Demand Service Manager or is it on a remote machine? _____

4. Type of emulation being used: TN3270_____ TN5250_____ VT_____ CICS_____ 3270 print _____ 5250 print_____ FTP_____

5. Are you using the default interface (the "green screen"), Screen Customizer/LE interface or the full Screen Customizer product?_____

6. If you are using Windows NT, Windows 2000, or Windows XP, are you logged onto the machine with administrative authority? _____

7. If your web browser is configured to use proxies, what are the proxy settings?

HTTP: _____

Socks: _____

Secure: _____

FTP: _____

Gopher: _____

WAIS: _____

8. Are there any messages posted in the Java Console?

To display the Java Console while using Netscape:

- Under Netscape 4.x, Select Communicator > Tools > Java Console from the main menu bar.

- Under Netscape 6, Select Tasks > Tools > Java Console from the main menu bar.

The Java Console appears in a separate window.

To display the Java Console while using Internet Explorer:

- Select Tools > Internet Options from the main menu bar.
- Click the Advanced tab.
- Scroll down to the Microsoft VM section and click in the checkbox next to Java Console Enabled (requires restart) to enable the Java Console.
- Click Apply.
- Click OK.
- Stop Internet Explorer and restart it.
- Select View > Java Console from Internet Explorer's main menu to view the Java Console. The Java Console window appears.

9. Does the problem occur regularly or only some of the time? _____
10. Does the problem occur with Netscape Navigator, Microsoft Internet Explorer, or both? _____
11. Does the problem fail on specific levels of the browser with specific JVM levels? _____
12. Does the problem occur for all users, on all operating systems or just specific operating systems? _____
13. Does the problem occur when you are logged on to the client workstation as an Administrator or user without restrictions to the directories or Windows registry? _____
14. Does the problem exist in both the Download and Cached clients? _____
15. What operating system are you using? _____

On a Windows platform, you can determine the operating system you are using by selecting Start > Settings > Control Panel > System. The first screen of the System selection displays information about your operating system

16. What browser versions are you using to run the Host On-Demand client:

INTERNET EXPLORER _____

NETSCAPE _____

You can determine the version of browser you are using by selecting HELP on the Browser toolbar and then selecting About Internet Explorer or About Netscape.

17. Does this problem occur on specific screens or all screens? _____

Steps to recreate:

18. Do you have an old version of the Cached client or Administration client installed?

If so, remove it by using the Remove Cached client function under Utilities on the HODMain.html page.

19. What type of security is being used? SSL or TLS only _____ Server Authentication _____ Client Authentication _____ Native Authentication _____ Express Logon _____
20. What type of certificate? CA _____ Self Signed _____
21. Type of Host On-Demand client: Cache _____ Download _____ DebugCache _____ DebugDownload _____
22. What type of Web server is being used? _____
23. What is the Web server's Name _____ Version _____ and release _____ ?

24. What operating system is being used for the Host On-Demand server? _____
25. What level of JVM is running on the machine where the Host On-Demand Service Manager is running?

To determine the JVM level, issue the command `Java -fullversion` at a command prompt _____

26. Is the Host on Demand Redirector being used? _____
27. Is the Host on Demand Configuration Servlet being used? _____
28. Is the HTML file being used a product of the Deployment Wizard? _____
29. What ports do the Host on Demand client and server use?
30. What TN3270/5250 server are you using? Name _____ Version _____ and release _____
31. Is the TN3270/5250 server on the same machine as the Host On-Demand server? _____
32. Describe the Network Environment:

33. Are you experiencing problems with 5250 host printing? Use the following checklist for contacting customer service. Check the following:
- a. Host On-Demand Version
 - b. Telnet server
 - c. Client platforms
 - d. What type of printer is being used ? (HP, Lexmark, etc)
 - e. Is it a local or networked attached printer?
 - f. How many users are experiencing this problem?
 - g. Are Customized Objects being used with 5250 printer sessions?
 - h. Is SSL being used with printer sessions?
 - i. How were the sessions created? (Deployment Wizard, etc.)
 - j. Has printing worked before now?
34. Are you experiencing problems with 3270 host printing? Use the following checklist for contacting customer service. Check the following:
- a. Host On-Demand Version
 - b. Telnet server
 - c. Client platforms
 - d. Browser and JVM level
 - e. Local or networked attached printers?
 - f. Are you trying to do a print screen?
 - g. What type of printer are you using? (HP, Lexmark, and so forth)
 - h. Are you using a PDT?
 - i. Are you using LUs?
 - If so, what type of LU (Explicit or Implicit)?
 - What type of server are you using for the LUs?
 - j. Are you using Screen Customizer?
 - k. Are you using SSL?
 - l. What platform are the clients using (such as Windows 95, 98, 2000, NT)?
 - m. Are you using associated printer sessions?

- n. Are you using Native windows printing?
- o. How many users are affected by this printer problem?
- p. What is the printer buffer size with in the Host On-Demand configuration sessions?
- q. Take a screen shot of the Host On-Demand session properties panel.
- r. Has printing worked before now?

Please include the following files (which contain information from the time the problem occurred):

- The Java Console from the Host On-Demand client.
- The NCoDServices.RAS.txt from the Hostondemand private directory, which is the Service Manager trace file and is located on the Host on Demand server.
- For zOS, standard in and standard out from the Host On-Demand JCL.
- Copies of the files created by the Host On-Demand Deployment Wizard. These files are located in the ..hostondemand\hod\hoddata\your_file_name\... directory, and include:
 - your_file_name.html
 - autoyour_file_name.html
 - params.txt
 - winfo.txt
 - preload.obj
 - policy.obj
 - cf*.cfg
 - udparms*.txt .
- The HODWIZARD.LOG, which is the Deployment Wizard log, located in the hostondemand\hod directory.
- Trace files that IBM Service has requested.

Understanding the OIA



The OIA (Operator Information Area) is the area at the bottom of the screen where session indicators and messages appear. Listed below are the session information fields, with an explanation for each.

Control Unit Status (Column 1)

M a connection to a Telnet server has been established

Connection Protocol (Column 2)

A the protocol is TCP/IP

System Available (Column 3)

***** the session is connected to an application program (LU-LU connection)

p the session is connected to a host, but not to an application (SSCP-LU connection)

? the session is not connected or bind received

Security (Column 4)

When session data is being encrypted, a **+** appears in this column

Session Shortname (Column 7)

A single character (a-z) identifies the host session.

Input Inhibited (Column 9-17)

X [] Time is required for the host system to perform a function (3270 session only). Please wait.

X SYSTEM The host system has locked your keyboard. Please wait.

X <-o-> You tried to enter, insert, erase, or delete a character when the cursor was in a protected area. Move the cursor to an unprotected position and retry the operation (3270 session only).

X -f You requested a function that is not supported in the current session.

X II An operator input error occurred (5250 session).

Communications Messages (Columns 19-26)

These messages are preceded by a broken lightning bolt if the session is using the IBM3270 font; otherwise, they are preceded by COMM or PROG.

Communications Check

These messages indicate a communications problem between Host On-Demand and the server or host to which it is trying to connect.

- [COMM 654](#)
- [COMM 655](#)
- [COMM 657](#)
- [COMM 658](#)
- [COMM 659](#)

- [COMM 662](#)
- [COMM 663](#)
- [COMM 664](#)
- [COMM 665](#)
- [COMM 666](#)

Program Check

These messages indicate that there is an error in the datastream sent from the host application.

- [PROG 750](#)
- [PROG 751](#)
- [PROG 752](#)
- [PROG 753](#)
- [PROG 754](#)
- [PROG 755](#)
- [PROG 756](#)
- [PROG 758](#)
- [PROG 759](#)
- [PROG 760](#)
- [PROG 761](#)
- [PROG 780](#)
- [PROG 797](#)
- [PROG 798](#)
- [PROG 799](#)

Cursor's current line and column number (Columns 75-80)

Comm 654

The session could not establish a connection to the Telnet3270E server because the specified LU name is not valid. The LU name may not be valid for the following reasons:

- The LU name is already in use by another session.
- The LU name is not defined at the Telnet server.
- The Telnet server does not support the LU type of the specified LU.
- The LU name is not compatible with the requested LU type. For example, the session type is Display, but the specified LU is a Printer.
- The Telnet server is unable to process this type of request. Contact your system administrator for help.
- An unknown error occurred during Telnet device-type negotiations. Contact your system administrator for help.

Ensure that your session's destination address, port, and LU name are correct. Also, ensure that your Telnet server is configured for the LU name that you are requesting. To determine which error condition is occurring, take a Transport Level 1 trace of your session startup.

Comm 655

- The socket connection to the Telnet server has been established and the session is waiting for negotiation to finish.

- The client has SSL off and has tried to connect to the server on an SSL port.

Comm 657

- The session is in the process of establishing the TCP/IP connection to the Telnet server.
- For SSL:
 - The client has SSL on and has tried to connect to the server on a non-configured port. You will first receive a brief COMM657, which changes to COMM659. If Auto-reconnect is enabled, the emulator will cycle in this pattern; otherwise, COMM659 remains.
 - The client has SSL on and has tried to connect to the server on a non-SSL port. You will first receive a COMM657, which changes to COMM659 after some time. If Auto-reconnect is enabled, the emulator cycles in this pattern; otherwise, it stays at COMM659.

When you close a session that displays COMM657, there may be some delay before it closes. The delay varies. If you are in a hurry, close the browser.

Comm 658

The session is initializing the TCP/IP connection for Telnet3270E.

Comm 659

- The Telnet TCP connection to the session has not succeeded or has failed.
 - The TCP/IP connection to the Telnet3270 server could not be established.
 - You clicked Disconnect on the Communication menu.
 - The Telnet server closed the TCP/IP connection either by application control or because it detected an error.
 - For 5250, the specified workstation ID is already in use, and the host closed the connection.

Ensure that your Telnet server and its port customization settings are correct. Also, ensure that your Telnet server is running and that it is configured correctly. To determine which error condition is occurring, take a Transport Level 1 trace when the error occurs.

● For SSL:

- The client has SSL off and has tried to connect to the server on a non-configured port.
- The client has SSL on and has tried to connect to the server on a non-configured port. You will first receive a brief COMM657, which changes to COMM659. If Auto-reconnect is enabled, the emulator will cycle in this pattern; otherwise, COMM659 remains.
- The client has SSL on and has tried to connect to the server on a non-SSL port. You will first receive a COMM657, which changes to COMM659 after some time. If Auto-reconnect is enabled, the emulator cycles in this pattern; otherwise, it stays at COMM659. The client has SSL on but cannot gain access to the key database on the server. This can happen if, for example, the database is not there, is corrupted, or does not have a password.

Comm 662

The server presented a certificate that was not trusted.

Comm 663

The server's certificate did not match its name. Because the session requested server authentication, the connection was refused.

Comm 664

A secure connection could not be completed.

Comm 665

The server's certificate is not yet valid.

Comm 666

The server's certificate has expired.

Prog 750

A 3270 command was received that is not valid.

Prog 751

A START FIELD EXTENDED, MODIFY FIELD, or SET ATTRIBUTE order was received which specified a character set that is not valid.

Prog 752

A SET BUFFER ADDRESS, REPEAT TO ADDRESS, or ERASE UNPROTECTED TO ADDRESS order was received which specified an address that is not valid.

Prog 753

One or more of the following conditions occurred:

- A READ MODIFIED, READ MODIFIED ALL, or READ BUFFER command that also contained data was received.
- A REPEAT TO ADDRESS or GRAPHIC ESCAPE order was received which specified a character set that is not valid.
- A START FIELD EXTENDED, MODIFY FIELD, or SET ATTRIBUTE order was received which specified an attribute value or character set that is not valid.

Prog 754

One of the following commands was received without the required parameters:

- SET BUFFER ADDRESS
- REPEAT TO ADDRESS
- ERASE UNPROTECTED TO ADDRESS
- START FIELD
- START FIELD EXTENDED
- MODIFY FIELD
- SET ATTRIBUTE
- GRAPHIC ESCAPE

Prog 755

A character code was received that is not valid.

Prog 756

A WRITE STRUCTURED FIELD command was received with a structured field that is not valid.

Prog 758

A SET REPLY MODE command was received with a mode that is not valid.

Prog 759

A WRITE STRUCTURED FIELD command was received with a structured field length that is not valid.

Prog 760

A WRITE STRUCTURED FIELD command was received with reserved fields that are not zero.

Prog 761

A WRITE STRUCTURED FIELD command was received with a partition identifier that is not valid.

Prog 780

An internal message was received with an incorrect direction.

Prog 797

SO was received; however, SO/SI are not paired correctly.

Prog 798

SO/SI or GRAPHIC ESCAPE was received in a DBCS field.

Prog 799

One or more of the following conditions occurred:

- Address points to the second byte of a DBCS character.

- A character attribute in a DBCS subfield is not valid.
- STOP address is not valid.
- General DBCS error.

Message Help



Click on a message number to view an explanation of the message and any action you need to take.

- [LOG001](#)
- [LOG002](#)
- [ECL0001](#)
- [ECL0002](#)
- [ECL0003](#)
- [ECL0004](#)
- [ECL0006](#)
- [ECL0007](#)
- [ECL0008](#)
- [ECL0009](#)
- [ECL0010](#)
- [ECL0011](#)
- [ECL0012](#)
- [ECL0030](#)
- [ECL0031](#)
- [ECL0032](#)
- [ECL0033](#)
- [ECL0034](#)
- [ECL0035](#)
- [ECL0036](#)
- [ECL0037](#)
- [ECL0038](#)
- [ECL0043](#)
- [ECL0076](#)
- [ECL0101](#)
- [ECL0102](#)
- [ECL0104](#)
- [ECL0105](#)
- [ECL0106](#)
- [ECL0126](#)
- [ECL0127](#)
- [ECL0128](#)
- [ECL0129](#)
- [ECL0130](#)
- [ECL0131](#)
- [ECL0132](#)
- [ECL0133](#)
- [ECL0134](#)
- [ECL0135](#)
- [ECL0136](#)
- [ECL0137](#)
- [ECL0138](#)
- [ECL0139](#)
- [ECL0140](#)
- [ECL0141](#)
- [ECL0142](#)
- [ECL0143](#)

[ECL0144](#)
[ECL0145](#)
[ECL0146](#)
[ECL0147](#)
[ECL0148](#)
[ECL0149](#)
[ECL0160](#)
[ECL0168](#)
[ECL0169](#)
[ECL0170](#)
[ECL0171](#)
[ECL0172](#)
[ECL0173](#)
[ECL0174](#)
[ECL0175](#)
[ECL0176](#)
[ECL0177](#)
[ECL0179](#)
[ECL0180](#)
[ECL0181](#)
[ECL0182](#)
[ECL0183](#)
[ECL0185](#)
[ECL0186](#)
[ECL0251](#)
[ECL0252](#)
[ECL0253](#)
[ECL0254](#)
[ECL0255](#)
[ECL0256](#)
[ECL0257](#)
[ECL0258](#)
[ECL0259](#)
[ECL0260](#)
[ECL0261](#)
[ECL0262](#)
[ECL0263](#)
[ECL0264](#)
[HOD0001](#)
[HOD0002](#)
[HOD0003](#)
[HOD0004](#)
[HOD0005](#)
[HOD0006](#)
[HOD0007](#)
[HOD0009](#)
[NSM0001](#)
[NSM0002](#)
[NSM0003](#)
[NSM0004](#)
[NSM0005](#)
[NSM0006](#)

[NSM0007](#)
[NSM0008](#)
[NSM0009](#)
[NSM0501](#)
[NSM0502](#)
[NSM1001](#)
[NSM1002](#)
[NSM1003](#)
[NSM1004](#)
[NSM1005](#)
[NSM1006](#)
[NSM1007](#)
[NSM1008](#)
[NSM1009](#)
[NSM1010](#)
[NSM1011](#)
[NSM1012](#)
[NSM1015](#)
[NSM1016](#)
[RDR0001](#)
[RDR0002](#)
[RDR0004](#)
[RDR0008](#)
[DIR0001](#)
[DIR0002](#)
[DIR0003](#)
[DIR0004](#)
[DIR0005](#)
[DIR0006](#)
[DIR0007](#)
[DIR0008](#)
[DIR0009](#)
[DIR0010](#)
[DIR0011](#)
[DIR0012](#)
[DIR0013](#)
[DIR0014](#)
[DIR0015](#)
[DIR0016](#)
[DIR0017](#)
[DIR0018](#)
[DIR0019](#)
[DIR0020](#)
[DIR0011](#)
[DIR0022](#)
[DIR0023](#)
[DIR0024](#)
[DIR0025](#)
[DIR0026](#)
[DIR0027](#)
[DIR0028](#)
[DIR0029](#)

[DIR0030](#)
[DIR0031](#)
[DIR0032](#)
[DIR0033](#)
[DIR0034](#)
[DIR0035](#)
[DIR0036](#)
[DIR0037](#)
[DIR0038](#)
[DIR0039](#)
[DIR0040](#)
[DIR0041](#)
[DIR0042](#)

LOG001

Explanation

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

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

User Action

Check to see if any reasons given above apply, or else contact your system administrator.

LOG002

Explanation

The Host On-Demand client is using a Configuration Servlet URL: `\n"%1\"` and is unable to contact the Host On-Demand Service Manager for one of the following reasons:

- The Configuration Servlet is not installed, is not operational or is not configured with the correct hostname and port number of the Service Manager.
- The client's ConfigServerURL parameter does not point to the Configuration Servlet or is missing the `\"/hod\"` extension from the end of the URL.
- A network problem has prevented the connection.
- The Service Manager is not started or is not operational.

User Action

Check to see if any reasons given above apply, or else contact your system administrator.

ECL0001 Internal Host Access Class Library program error.

Explanation

The Host Access Class Library has encountered an internal problem.

User Action

If there are other messages preceding this one, try to correct any indicated problems. Also ensure you have the latest fixes applied for this product. If the problem persists, follow the directions in the README file for reporting product problems.

ECL0002 A Host Access Class Library event-error occurred.

Explanation

The Host Access Class Library encountered a problem during event generation. This is a notification message only. There should be other messages logged that provide more details.

User Action

Look for other messages in the message log to determine the cause of this error.

ECL0003 Error updating field at %1. The field is protected.**Explanation**

You attempted to write to a protected field, which is not allowed.

User Action

If the error was generated during normal use of Host On-Demand, follow the directions in the README file to report the problem. If the error was generated by another applet, application or product that uses the Emulator Class Library, contact the originator of the applet, application or product to report this problem.

ECL0004 No field found at position %1.**Explanation**

No field was found at the specified location. This was probably the result of an internal error.

User Action

If the error was generated during normal use of Host On-Demand, follow the directions in the README file to report the problem. If the error was generated by another applet, application or product that uses the Emulator Class Library, contact the originator of the applet, application or product to report this problem.

ECL0006 Browser version is not valid.**Explanation**

Host On-Demand could not create the requested session because the current browser or execution environment does not support all the needed functions. Host On-Demand must run in a browser or execution environment that fully supports JVM version 1.1.

User Action

Obtain the latest version of the browser from your system administrator or the company that supplies it.

ECL0007 Server %1 could not be authenticated for this connection.**Explanation**

A secure connection was requested with an authenticated server. however, the server could not be authenticated.

User Action

Check with your network security personnel to see if server authentication is necessary for this connection. If server authentication is not necessary, do not request server authentication when defining the session. If server authentication is necessary, the common name in the subject field of the server's certificate must be the same as the server's network name.

ECL0008 Could not create a secure connection to server %1.**Explanation**

Host On-Demand attempted a secure connection to the server, but the attempt was not successful.

User Action

Make sure the server you are trying to connect to supports Transport Layer Security (TLS) 1.0 secure connections.

It is also possible that the server does not have enough capacity to accept another secure connection at this time. If this is the case, try the connection when the server is not as busy.

ECL0009 Server "%1" presented a certificate that was not trusted.

Explanation

Host On-Demand attempted a secure connection to the server, but the certificate the server sent to identify itself was not issued by a trusted CA.

User Action

To complete the connection you can extract the appropriate server certificate and add it to the list of trusted CAs. To view the certificate, choose Security from the Communications pull-down menu of the emulator menu bar. You should see information about the certificate that was not trusted.

If Show Issuer Certificate is not grayed out, click that button to display the issuer of the server's certificate, and extract the issuer's certificate to a file. If Show Issuer Certificate is grayed out, click Extract to save the server's certificate to a file. You can then add it to the list of trusted CAs (locally-installed clients) or send it to your Host On-Demand administrator to add to the CustomizedCAs.class file on the server.

Certificates received over the Internet can be forged. The safest way to verify the authenticity of a certificate is to display the finger print of the certificate you have received, and then contact the administrator of the server you are connecting to and ask for the finger print of the certificate on the server. If the finger prints match, you have an authentic certificate and may safely add it to the list of trusted CAs.

ECL0010 Parameter %1 is not valid. The value is %2.

Explanation

The value specified for the given parameter is not valid for one of the following reasons:

- The value is out of the permitted range.
- The value is not recognized.
- The value is not valid for the current session type.

User Action

If you supplied the value for this parameter, refer to the Emulator Class Library reference to verify that you are using a valid value.

If the error is generated during normal use of Host On-Demand, follow the directions in the README file to report the problem. If the error is generated by another applet, application or product that uses the Emulator Class Library, contact the originator of the applet, application or product to report this problem.

ECL0011 Parameter %1 is not valid. The value is null.

Explanation

The value specified for the given parameter is not valid because it is null.

User Action

If you supplied the value for this parameter, refer to the Emulator Class Library reference to verify that you are using a valid value.

If the error is generated during normal use of Host On-Demand, follow the directions in the README file to report the problem. If the error is generated by another applet, application or product that uses the Emulator Class Library, contact the originator of the applet, application or product to report this problem.

ECL0012 Parameter %1 is not valid. The data contains an incomplete or unrecognized mnemonic keyword.

Explanation

The value specified for the given parameter is not valid because it contains a mnemonic keyword that is either incomplete or unrecognized.

User Action

If you supplied the value for this parameter, refer to the Emulator Class Library reference to verify that you are using a valid value.

If the error is generated during normal use of Host On-Demand, follow the directions in the README file to report the problem. If the error is generated by another applet, application or product that uses the Emulator Class Library, contact the originator of the applet, application or product to report this problem.

ECL0030 The server certificate from host %1 is not yet valid.

Explanation

Before establishing a secure session, the server must present a certificate to the client that is valid only for a specified period of time. In the aborted connection, the certificate that the host presented will be valid at a future date, but is not currently valid.

User Action

First, make sure the client configuration has the correct date, time, and time zone. If any of these values are wrong, make the appropriate corrections.

If the client is correct and you are using a self-signed certificate generated on the server, check the date, time, and time zone of the server. If any of these are wrong, make the appropriate corrections and re-create the self-signed certificate.

ECL0031 The server certificate from host %1 has expired.**Explanation**

Before establishing a secure session, the server must present a certificate to the client that is valid only for a specified period of time. In the aborted connection, the certificate that the host presented was valid at a past date, but is not currently valid.

User Action

First, make sure the client configuration has the correct date, time, and time zone. If any of these values are wrong, make the appropriate corrections.

If the client is correct and you are using a self-signed certificate generated on the server, check the date, time, and time zone of the server. If any of these are wrong, make the appropriate corrections and re-create the self-signed certificate.

If the client is correct and you are using a CA-signed certificate, check the validity of the certificate. If the validity period has expired, you may need to renew the certificate with the CA.

ECL0032 Server %1 requested a client certificate, but the client-certificate information is incomplete.**Explanation**

While attempting to negotiate a secure connection, the server requested a client certificate. Before Host On-Demand can send a certificate, more information must be supplied by the user.

User Action

This message will cause the user to be prompted for certificate information. The user can choose not to send a certificate, or can supply the location and password of a valid client certificate in PKCS12 format.

ECL0033 Client certificate was not found at %1.**Explanation**

When prompted for a client certificate, the user entered a URL or path and file name that could not be found.

User Action

Ensure that the name of the certificate was entered correctly and is accessible to the browser.

ECL0034 Certificate password was incorrect or certificate found at %1 was corrupted.**Explanation**

When prompted for a client certificate, the user entered a certificate and password, but the certificate could not be decrypted with the password. This indicates that either the password is incorrect, or the certificate file has been corrupted.

User Action

Ensure that the name of the certificate and its password were entered correctly. If they were, compare the certificate file to a backup copy. If the two files are the same, report the error to the person who created the file.

ECL0035 Server %1 requested a client certificate and the certificate found at %2 was presented, but the server refused the connection.**Explanation**

When prompted for a client certificate, the user entered a valid certificate and password, and the certificate was decrypted and sent to the server. However, the server refused the connection.

User Action

If another client certificate is available, enter its location and password when prompted. If all available certificates have been presented and rejected, you can attempt to connect without a certificate. The server may allow the connection at a lower privilege level. If the server still refuses the connection, contact the server's administrator.

ECL0036 Unable to initialize the security system; error code [%1], error message [%2].

Explanation

The Host On-Demand libraries that implement client authentication could not be found or initialized.

User Action

Re-install the Host On-Demand product. If the error still occurs, contact Host On-Demand service and report the error information.

ECL0037 Server %1 does not support Telnet-negotiated security.

Explanation

Telnet-negotiated security uses the Transport Layer Security (TLS) protocol and Telnet-negotiated security. Servers that support these functions respond IAC DO STARTTLS during the Telnet negotiations. Host On-Demand has received IAC DONT STARTTLS from the server or an invalid response to the IAC WILL STARTTLS. The connection with the server is terminated.

User Action

Check that the server supports TLS. If your server does not support this function, then select No for Telnet-negotiated on the Security tab of the session configuration. If your server does support this function, verify the server's port is configured properly to receive the TLS protocol negotiations.

ECL0038 Unable to write to %1.

Explanation

The user requested that a URL or local file be created or saved, but the request failed.

User Action

Ensure that the URL or file was typed correctly, and that you have write permission for the file. Most browsers do not support writing to a URL.

ECL0043 Server %1 requested a client certificate, but no client certificate has been provided.

Explanation

While attempting to negotiate a secure connection, the server requested a client certificate. However, the session has been configured not to send a client certificate to the server. The server refused the connection.

User Action

If you have a client certificate, then the session must be configured to send that certificate when it is requested by the server. To do this, select Yes for Send a Certificate on the Security tab of the session configuration. You can also specify the default location of the PKCS12 file containing the client certificate. If you do not have a certificate, contact the system administrator of the server you are attempting to connect to.

ECL0076 Sequence %1 is not valid or is unsupported.

Explanation

This message might appear during a VT emulator session. This message is logged by the DataStream component if a VT host application sends a sequence that HOD does not support (for example, ansi color sequences), or if it sends a VT sequence that is not valid.

User Action

Receiving these sequences may not affect screen output. If the application is acting abnormally, turn on trace level 1 for the DataStream component and rerun the scenario. Submit the trace/log files to the VT Host application administrator.

The administrator can use the trace files to debug an erroneous program. The administrator may determine that the application requires a terminal type different than VT220/VT100/VT52.

ECL0101 Failed to connect to server/host %1 and port %2.

Explanation

A socket connection failed to the specified host or server and port.

User Action

Verify that the Destination Address and Destination Port as specified in the Connection configuration are correct. Check that the host is operational and can be reached.

If this is an SLP connection and there is no hostname, then no servers responded indicating support of service. Refer to message ECL0102 for more information. If this is an SLP connection and there is a hostname, check that the server is operational for TN3270 or TN5250.

ECL0102 Failed to find any SLP servers.

Explanation

No servers responded to the SLP request within the specified timeout.

User Action

Check that the Scope on the Advanced configuration panel matches the Scope of an available server in the network. If Enable Security on the Security configuration is Yes, verify that there is an available server within the specified scope that supports either TLS version 1.0 or SSL version 3.0.

If there is an SLP iSeries name specified on the Connection configuration, verify that it is a valid, fully qualified CP name and that there is an available server within the specified scope that links to that iSeries.

If the network is slow, increment the Maximum Wait Time.

Verify the Browser supports Multicasting.

If on a Token Ring, verify that the server and the client are both using the same IP multicasting address mapping method: either the all rings broadcast address or the assigned functional address (rfc 1469).

ECL0104 Exception, unable to load class %1.

Explanation

Host On-Demand was unable to load the Java class with name %1.

User Action

Ensure that you are running Host On-Demand in the proper environment. For example, if running in a web browser, check to ensure that the web browser meets Host On-Demand prerequisite requirements.

ECL0105 Exception, unable to instantiate class %1.

Explanation

Host On-Demand was unable to create an instance of the Java class with name %1.

User Action

Ensure that you are running Host On-Demand in the proper environment. For example, if running in a web browser, check to ensure that the web browser meets Host On-Demand prerequisite requirements.

ECL0106 Exception, illegal access for class %1.

Explanation

Host On-Demand attempted to access the Java class with name %1 but was prevented from doing so due to security reasons.

User Action

Ensure that you are running Host On-Demand in the proper environment. For example, if running in a web browser, check to ensure that the web browser meets Host On-Demand prerequisite requirements.

ECL0126 An exception was detected at reference location %1.**Explanation**

An exception condition was detected by the file transfer program. The reference location identifies where in the program the exception was detected.

User Action

This message is usually associated with a program error. Turn on trace level 1 for the ECL_xfer and Transport components and rerun the scenario. Submit the trace/log files to IBM support.

ECL0127 File transfer complete.**Explanation**

A file transfer was successfully completed.

User Action

No action is required.

ECL0128 Error writing file to the host: file transfer canceled.**Explanation**

The file could not be written to the host.

User Action

Check to make sure you have enough space and that the disk is still online. Correct any problems and try to transfer the file again.

ECL0129 Error reading file from the host: file transfer canceled.**Explanation**

The file could not be read from the host.

User Action

Check to make sure you have enough space and that the disk is still online. Correct any problems and try to transfer the file again.

ECL0130 Required host storage is unavailable: file transfer canceled.**Explanation**

Adequate host resources are not available to store the file.

User Action

Create more room on the host by deleting files or adding space, then try to transfer the file again.

ECL0131 Incorrect request code: file transfer canceled.**Explanation**

An incorrect request was issued to the host file transfer program.

User Action

Run a trace and report the results to IBM.

ECL0132 Incorrect or missing TSO data set: file transfer canceled.

Explanation

An incorrect data set was specified for the transfer.

User Action

Make sure you specified the correct file name, then try to transfer the file again.

ECL0133 Missing or incorrect CMS file identifier: file transfer canceled.

Explanation

An incorrect CMS file identifier was specified.

User Action

Make sure the CMS file identifier is correct, then try to transfer the file again.

ECL0134 Incorrect option specified: file transfer canceled.

Explanation

An incorrect host file transfer option was specified.

User Action

Make sure the options specified for this transfer are correct, then try to transfer the file again. If the file transfer still fails, contact the administrator of the host transfer program for assistance.

ECL0135 Error reading from or writing to host disk: file transfer canceled.

Explanation

The host computer detected an error reading or writing to disk.

User Action

Check to make sure you have enough space and that the disk is still online. Correct any problems and try to transfer the file again.

ECL0136 Only one of TRACKS, CYLINDERS, AVBLOCK allowed: file transfer canceled.

Explanation

Only one media division can be specified.

User Action

TRACKS, CYLINDERS, or AVBLOCKS are not specified by HftpTransfer programmatically. If these are specified manually, please be sure that such specification is in accordance with the host file transfer program.

ECL0137 CMS file not found: file transfer canceled.

Explanation

The requested file was not found.

User Action

Correct the specification of the file you want to transfer, then try to transfer the file again. If the file transfer still fails, contact the administrator of the host transfer program for assistance.

ECL0138 CMS disk is read-only: file transfer canceled.

Explanation

Write access is required but is not available to perform the requested operation.

User Action

Obtain the appropriate write access for the requested operation, then try to transfer the file again. If the file transfer still fails, contact the

administrator of the host transfer program for assistance.

ECL0139 CMS disk is not accessed: file transfer canceled.

Explanation

The requested CMS mini-disk is not accessed.

User Action

Obtain appropriate access for the requested operation, then try to transfer the file again. If the file transfer still fails, contact the administrator of the host transfer program for assistance.

ECL0140 CMS disk is full: file transfer canceled.

Explanation

The requested CMS mini-disk is full.

User Action

Allocate additional storage or delete files on the target disk to provide storage to support the requested transfer, then try to transfer the file again. If the file transfer still fails, contact the administrator of the host transfer program for assistance.

ECL0141 Host program error: file transfer canceled.

Explanation

An unspecified error was detected by the host file transfer program.

User Action

Try to transfer the file again. If file transfer still fails, run a trace and report the results to IBM.

ECL0142 Host operation failed to complete within timeout period.

Explanation

The host did not respond within the specified timeout period. The timeout period is applied to the smallest increment of processing that indicates the host is attempting to service the request. For example, to download a large file the host transfers many separate buffers of data. The timeout period is applied separately to each buffer transferred.

It is possible that:

- Access to the host has been lost.
- The system is heavily loaded and response is being delayed.
- The timeout period is too short.
- The host is not in the correct state to perform file transfer.

User Action

In some cases, you can extend the timeout period to circumvent this problem. Otherwise, it will be necessary to determine why the host response is delayed and apply appropriate corrective action. Change the timeout parameter to a higher value.

ECL0143 Session with host does not exist. Please close file transfer windows.

Explanation

The host session has been closed or lost. File transfer is not possible.

User Action

Stop file transfer by closing the file transfer windows. To use the file transfer function, start a new session.

ECL0144 Unable to open the local file for reading.

Explanation

The file transfer facility attempted to read a file on the local file system but could not open the file. The filename or filepath may not have been entered correctly. In the case of a removable disk, the disk may not be installed.

User Action

Verify that the file is correctly specified and that media is correctly mounted.

ECL0145 Unable to open the local file for writing.

Explanation

The file transfer facility attempted to open a file for writing, but could not open the file. The specified file may already exist and be write-protected, removable media may not be installed or may be write-protected, or the media may be full.

User Action

Confirm that the correct filepath is specified. Confirm that the media is installed and is not write-protected.

ECL0146 Error while reading from the local filesystem.

Explanation

This error could be caused by a hardware or media failure. In the case of removable media, the media may have been inadvertently dismounted during a transfer operation; for example, someone opened the disk drive.

User Action

Confirm that the media is properly installed.

ECL0147 Error while writing to the local filesystem.

Explanation

The disk has become filled to capacity or a hardware failure has occurred. In the case of removable media, the disk may have been inadvertently removed.

User Action

Verify that the media is properly mounted. Verify that adequate disk capacity is available. It may be necessary to remove some files to make room for the new files you are downloading.

ECL0148 File transfer canceled by an external caller.

Explanation

The file transfer was canceled by a call to ECLXfer.Cancel().

User Action

No action is required.

ECL0149 Cannot transfer a zero-length file: file transfer canceled.

Explanation

The PC file is of size zero bytes and can't be transferred to the host.

User Action

Specify a PC file that is not empty.

ECL0160 Error creating PDT.

Explanation

The compiler cannot create an empty PDT object.

User Action

Contact IBM service.

ECL0168 Could not open the PDT Compiler log.

Explanation

The compiler cannot open the log file pdtc.log.

User Action

Make sure there is enough disk space to open the file.

ECL0169 The description must begin with a non-blank character.

Explanation

The printer description begins with a blank character.

User Action

Type a printer description that begins with a character other than blank.

ECL0170 A valid description must be entered.

Explanation

You tried to compile without typing a printer description.

User Action

Enter a valid printer description.

ECL0171 You must select a valid PDF file.

Explanation

You attempted to compile before selecting a PDF from the choice box.

User Action

Select the PDF you want to compile from the choice box.

ECL0172 The description may not begin with KEY.

Explanation

You have typed a printer name description that begins with KEY. KEY is reserved by IBM.

User Action

Enter a printer name description that does not begin with KEY.

ECL0173 The description may not be blank.

Explanation

The printer description field is blank.

User Action

Enter a printer description.

ECL0174 Compiler failed--internal error.

Explanation

The PDT compiler failed.

User Action

Contact IBM service.

ECL0175 Error reading macro definition.

Explanation

An error was encountered while reading the PDF from disk to obtain macro definitions.

User Action

Make sure the disk is online and available.
Open the PDF with an editor and make sure that it is valid. Correct any errors.

ECL0176 Warning: Unrecognized parameter defined:

Explanation

A parameter defined in the PDF is not recognized by the PDT Compiler. It is possible you have modified the PDF to support a custom function that requires this parameter.

User Action

Usually, no action is required.

ECL0177 Command name unknown:

Explanation

The PDF contains a command definition that is not recognized by the compiler.

User Action

Remove the command definition from the PDF.

ECL0179 Error converting decimal string to byte.

Explanation

An attempt was made to code a decimal string larger than 255, which is the maximum value that can be stored in 1 byte.

User Action

Correct the failing definition in the PDF.

ECL0180 EQU is not the second token in the macro.

Explanation

A macro definition does not EQU as the second token.

User Action

Add EQU to the PDF definition.

ECL0181 Bad token detected:

Explanation

A command definition contains a token for which there is no valid macro definition.

User Action

Correct the failing definition in the PDF.

ECL0182 Could not open PDF file:

Explanation

The compiler can not open the selected PDF.

User Action

Make sure the selected PDF exists.

ECL0183 Compilation failed.

Explanation

The compiler detected errors.

User Action

Review the errors detected by the compiler.
Correct the failing definitions in the PDF and try to compile again.

ECL0185 Less than 3 tokens in macro definition.

Explanation

A macro definition has less than 3 tokens.

User Action

Correct the failing definition in the PDF.

ECL0186 Macro name length not 3.

Explanation

The first token of a macro definition is not 3 characters in length.

User Action

Correct the failing definition in the PDF.

ECL0251 Unable to contact the host.

Explanation

Unable to get a connection to the host.

User Action

Make sure that the host is running and that you are able to ping it.

ECL0252 Invalid host-file name. Use the correct format: LibraryName/FileName OR LibraryName/FileName(MemberName) OR /Dir1/.../DirX/FileName

Explanation

An incorrect host-file name was specified.

User Action

Specify the host file in any of the following formats:

- LibraryName/FileName
- LibraryName/FileName(MemberName)
- /Dir1/.../DirX/FileName

The file name **QGPL/QCLSRC** is equivalent to **/QSYS.LIB/QGPL.LIB/QCLSRC.FILE** in IFS format. The file name **QGPL/QCLSRC(README)** is equivalent to **/QSYS.LIB/QGPL.LIB/QCLSRC.FILE/README.MBR** in IFS format.

ECL0253 Host file already exists: file transfer canceled.

Explanation

The host file already exists and the transfer option NEW was specified to avoid over-writing the existing file.

User Action

Specify a file that does not exist.

ECL0254 Host file does not exist: file transfer canceled.

Explanation

The host file does not exist.

User Action

Specify an existing host file.

ECL0255 PC file already exists: file transfer canceled.

Explanation

The PC file already exists and the transfer option NEW was specified to avoid over-writing the existing file.

User Action

Specify a file that does not exist.

ECL0256 PC file does not exist: file transfer canceled.

Explanation

The PC file does not exist.

User Action

Specify an existing PC file.

ECL0257 The selected host-file type is not supported.

Explanation

The selected host file can't be transferred to the host. Only iSeries objects of the type *FILE are supported under the QSYS library file system. Also, among the iSeries *FILE objects, only the file types PF-DTA (Physical Data File), PF-SRC (Source Physical file) and SAVF are supported.

User Action

Specify a valid host file.

ECL0258 Only binary mode allowed for transferring iSeries SAVF files.

Explanation

For transferring SAVF files to the iSeries, the transfer mode must be binary.

User Action

The transfer options ASCII, JISCII or UNICODE should not be specified for transferring SAVF files to the iSeries.

ECL0259 Unable to open the host file for writing.

Explanation

The host file cannot be created or changed.

User Action

Make sure that the user has authority to create or change the file.

ECL0260 Unable to open the host file for reading.

Explanation

The host file cannot be read.

User Action

Make sure that the user has authority to read the file.

ECL0261 Transfer error: %1

Explanation

Unable to complete the requested transfer operation.

User Action

If you are performing 5250 File Transfer and if an error message ID is included in the message (such as CPF9999), you can get more help by using the CL command DSPMSGD on aniSeries system. Also, if you get any of the following error messages when performing 5250 File Transfer, please refer to the *Planning, Installing, and Configuring Host On-Demand* guide and make sure that you followed the setup instructions correctly. You could still get any of the following messages if the host name is NOT the actual final destination address of the 5250 host. The default file transfer settings of the Host On Demand session can be changed to correctly indicate the actual final destination address of the 5250 host. For HACL applications, the transfer option DSTADDR can be used to set the final destination address for file transfer.

- ECL0261: Transfer error: Connection refused
- ECL0261: Transfer error: Server socket not accepting.: An unknown problem has occurred.
- ECL0261: Transfer error: SOCKS server cannot connect to identd

If you receive a ECL0261: Transfer error;security.fd.write when using the Host On-Demand Proxy Server service to perform AS/400 File Transfer, add ha5250xn.jar to your start up HTML file as follows:

```
<APPLET archive="hod.jar, ha5250xn.jar, sccbase.jar"
CODE="com.ibm.eNetwork.HOD.HostOnDemand.class" WIDTH=584 HEIGHT=450>
<PARAM NAME=cabinets VALUE=hod.cab,sccbase.cab>
<PARAM NAME=BookmarkPage VALUE=AutoHOD.html>
```

If you get the following message, please make sure that the environment variable CLASSPATH is set to nothing, before invoking 5250 File Transfer.

- ECL0261: Transfer error: sun.io.ByteToCharSingleByte: field byteToCharTable Ljava/lang/String; not found
-

ECL0262 Security error: %1

Explanation

Unable to log on to the host.

User Action

Specify a valid user ID and password to log on to the host.

ECL0263 Transfer incomplete. Only %1 bytes transferred.

Explanation

Only part of the file has been transferred.

User Action

Try to transfer the file again. If it still fails, run a trace and report the results to IBM.

ECL0264 Unable to convert data in UNICODE mode: the current version of the Java VM is not capable of handling %1 encoding.

Explanation

The current version of the Java Virtual Machine is not capable of handling the specified encoding.

User Action

Upgrade the Java VM to the latest version and check whether it can support the specified encoding.

HOD0001 Exception, unable to load class %1.

Explanation

Host On-Demand was unable to load the Java class with name %1.

User Action

Ensure that you are running Host On-Demand in the proper environment. For example, if running in a web browser, check to ensure that the web browser meets Host On-Demand prerequisite requirements.

HOD0002 Exception, unable to instantiate class %1.

Explanation

Host On-Demand was unable to create an instance of the Java class with name %1.

User Action

Ensure that you are running Host On-Demand in the proper environment. For example, if running in a web browser, check to ensure that the web browser meets Host On-Demand prerequisite requirements.

HOD0003 Exception, illegal access for class %1.

Explanation

Host On-Demand attempted to access the Java class with name %1 but was prevented from doing so due to security reasons.

User Action

Ensure that you are running Host On-Demand in the proper environment. For example, if running in a web browser, check to ensure that the web browser meets Host On-Demand prerequisite requirements.

HOD0004 Tracing for %1 set to level %2.

Explanation

Tracing for the %1 component of Host On-Demand has been set to level %2.

User Action

No action is required. This is an informational message.

HOD0005 Internal error occurred: %1.

Explanation

Host On-Demand experienced an unexpected error of type %1.

User Action

If there are other messages preceding this one, try to correct any indicated problems. Also ensure you have the latest fixes applied for this product. If the problem persists, following the directions in the README file for reporting product problems.

HOD0006 Unable to initialize tracing for %1.

Explanation

Host On-Demand was unable to start tracing for the %1 component.

User Action

Look in the message log for other error messages that indicate why tracing could not start.

HOD0007 Cannot find the selected code page resource. The default code page will be used.

Explanation

Host On-Demand was unable to find the code page conversion tables for the selected code page. Code page 037 will be used.

User Action

Make sure you installed the correct Host On-Demand for the code page you want to use.

HOD0009 The %1 function cannot be performed because of browser security restrictions.

Explanation

While attempting to perform the function or task that you requested, Host On-Demand was unable to access a related Java function because of security restrictions imposed by the browser. Either you did not grant the necessary security permissions (if prompted to do so), or your browser level or settings do not allow the security access needed by Host On-Demand.

User Action

Refer to the Host On-Demand Administrator's Guide to determine if you are running the correct level of browser or if you have the correct browser security settings.

NSM0001 Starting...

Explanation

The On-Demand Service Manager is starting.

User Action

No action is required. This is an informational message.

NSM0002 Listening on port %1.

Explanation

The On-Demand Service Manager is listening on the identified port.

User Action

No action is required. This is an information message.

NSM0003 Waiting for requests...

Explanation

The On-Demand Service Manager is waiting for requests.

User Action

No action is required. This is an information message.

NSM0004 Connection request received from %1.

Explanation

The On-Demand Service Manager has received a connection request from a client with the identified host name.

User Action

No action is required. This is an information message.

NSM0005 Service, %1, loaded.

Explanation

The On-Demand Service Manager has successfully loaded the identified service from the NSMprop file.

User Action

No action is required. This is an information message.

NSM0006 Service, %1, started.

Explanation

The On-Demand Service Manager has successfully started the identified service.

User Action

No action is required. This is an information message.

NSM0007 Service, %1, stopped.

Explanation

The On-Demand Service Manager has stopped the thread for the identified service.

User Action

No action is required. This is an information message.

NSM0008 Class, %1, loaded.

Explanation

The On-Demand Service Manager has successfully loaded the identified class.

User Action

No action is required. This is an information message.

NSM0009 <<< Loading default services >>>

Explanation

The On-Demand Service Manager has loaded the default services. **It has NOT loaded those services located in the NSMprop file.**

User Action

Check that the NSMprop exists and is in the correct directory. Look in the message log for other error messages that indicate why the services were not loaded from the NSMprop file.

NSM0501 Class, %1, not loaded. Exception caught: %2.

Explanation

The On-Demand Service Manager caught an exception while trying to load the identified class. Since the On-Demand Service Manager will try to load all the classes in the NSMprop file specifying autostart=yes, this may or may not be an error.

User Action

Check with the system administrator to see if the service associated with the unloaded class is required.

NSM0502 The service, %1, is not known or has not been loaded.

Explanation

The On-Demand Service Manager received a request for an unknown service.

User Action

If the request is from a user application, check for correct syntax. If the request is from another IBM application, look in the message log for other error messages that indicate why the service was not loaded.

(NSM1001) An error occurred creating ServerSocket: %1.

Explanation

The On-Demand Service Manager noted an exception while it was creating the server socket used to listen for requests. One possible cause is that another application is already using the port that the On-Demand Service Manager is trying to create a socket for.

User Action

If the exception indicates that the address is in use, stop any other applications using port 8989; otherwise, report the error to your system administrator.

NSM1002 An error occurred listening for requests.

Explanation

The On-Demand Service Manager noted an exception while it was listening for requests. One possible cause is that the port upon which On-Demand Service Manager was listening closed unexpectedly.

User Action

Restart the On-Demand Service Manager. If the problem persists, report the error to your system administrator.

NSM1003 An error occurred closing a socket: %1.

Explanation

The On-Demand Service Manager noted an exception while it was closing a socket.

User Action

Check the log for other socket problems and report the error to your system administrator.

NSM1004 The service, %1, has a dependency on %2, but it was not found.

Explanation

The On-Demand Service Manager received a request to start the first named service, which depends on the second named service being active; however, the second named service was not found.

User Action

Check the NSMprop file to determine if the second named service is one of the services loaded by On-Demand Service Manager. If it is, check the message log for errors indicating why the service was not loaded. Correct the NSMprop file and restart the On-Demand Service Manager.

NSM1005 The service, %1, has a dependency on %2, but it could not be started.

Explanation

The On-Demand Service Manager received a request to start the first named service which depends on the second named service being active; however, the second named service could not start.

User Action

Check the message log for errors indicating why the second named service did not start.

NSM1006 The service, %1, has a dependency on %2, but it has not been started.

Explanation

The On-Demand Service Manager received a request to start the first named service which depends on the second named service being active; however, the second named service did not start and has an autostart value of **NO**.

User Action

In the NSMprop file, change the autostart value of the second named service to **YES**.

NSM1007 (NSM1007) The initialize method of service, %1, returned false; service not started.

Explanation

The On-Demand Service Manager noted that while processing a request to start the indicated service, the service returned a value of false from its initialize method. This indicates that the service should not start.

User Action

Check the message log and see if the service logged any messages indicating why it did not start. Correct these conditions and try to start the service again.

NSM1008 An error occurred starting service, %1. Exception caught: %2.

Explanation

The On-Demand Service Manager noted an exception caused by the indicated service while the service was starting.

User Action

Correct the problem with the service and try the command again.

NSM1009 An error occurred stopping service, %1. Exception caught: %2.

Explanation

The On-Demand Service Manager noted an exception caused by the indicated service while the service was stopping.

User Action

Correct the problem with the service and try the command again.

NSM1010 An error occurred opening an input or output stream: %1.

Explanation

The On-Demand Service Manager noted an exception while it was opening a client's input or output stream. This might occur if the client closes the connection before the service manager has a chance to process its request.

User Action

Determine if the client is closing the connection too quickly and correct this condition; otherwise, report the error to your system administrator.

NSM1011 An error occurred receiving data: %1.

Explanation

The On-Demand Service Manager noted an exception while it was receiving data from a client's input stream. This might occur if the client closes the connection before the service manager has a chance to receive all the data.

User Action

Determine if the client is closing the connection too quickly and correct this condition; otherwise, report the error to your system administrator.

NSM1012 An error occurred sending data: %1.

Explanation

The On-Demand Service Manager noted an exception while it was sending data to a client. This might occur if the client closes the connection before the service manager has a chance to send all the data.

User Action

Determine if the client is closing the connection too quickly and correct this condition; otherwise, report the error to your system administrator.

NSM1015 The file, %1, was not found.

Explanation

The On-Demand Service Manager cannot find the indicated file. If the file is **NSMprop**, the service manager will load its default services. If the file is **NCoDServices.RAS.txt**, no message log is returned for viewing from the administration panel.

User Action

Verify that the indicated file is in the correct directory and is not corrupted. The **NSMprop** file should be in the `..lib` directory and the **NCoDServices.RAS.txt** file should be in the `..private` directory.

NSM1016 An error occurred accessing file, %1. Exception caught: %2.**Explanation**

The On-Demand Service Manager encountered an error while processing the indicated file. If the file is **NSMprop**, the service manager will load its default services. If the file is **NCoDServices.RAS.txt**, no message log is returned for viewing from the administration panel.

User Action

Verify that the indicated file is not corrupted and that no other application is accessing the file.

RDR0001 Could not establish connection to configuration server.**Explanation**

The Redirector could not connect to the configuration server to read configuration data.

User Action

Check to make sure that the IBM SecureWay On-Demand Service Manager is started.

RDR0002 No configuration data present.**Explanation**

The Redirector was started but has not been configured.

User Action

The redirector must be configured before you can use it. If you are not using the Redirector, ignore this message.

RDR0004 An error occurred accessing the key database file.**Explanation**

The Redirector could not access the key database file.

User Action

Using the Key-Management utility, check the following:

- The file `HODServerKeyDb.kdb` exists in the `ondemand\bin` directory.
 - The password for `HODServerKeyDb.kdb` has been stashed to `HODServerKeyDb.sth` in the `ondemand\bin` directory.
 - `HODServerKeyDb.kdb` contains a personal certificate which has been set as the default.
 - The validity period of the default personal certificate has not expired.
-

RDR0008 Native library failed to load, indicating this Redirector does not support TLS.**Explanation**

In order to support TLS sessions, the Redirector must load a native library to implement security functions. This library is only available on Windows NT, Windows 2000, and AIX platforms. The failure to load this library indicates that this server does not support TLS sessions.

User Action

If the Redirector is running on a platform that does not support TLS, then no action is necessary. If the Redirector is running on a platform that supports TLS, re-install the product. If the problem persists, contact an IBM service representative.

DIR0001 File does not exist: %1.

Explanation

The file specified cannot be found.

User Action

Verify that the file exists in the directory specified.

DIR0002 File cannot be opened: %1.

Explanation

The file cannot be opened.

User Action

Verify that the file is readable.

DIR0003 Invalid number of input parameters.

Explanation

There are three required parameters to start the DirUtil application: filename, admin, password.

User Action

Verify that filename, admin, and password have been specified.

DIR0004 Invalid file extension: %1. The valid extension is .xml.

Explanation

The filetype must be .xml. The DirUtil application parses the document as a valid xml document, checks for errors and validates the document.

User Action

Verify that the filetype is .xml when the document contains xml. See the online help for the valid xml file format.

DIR0005 The administrator ID specified is not valid.

Explanation

The ID specified for the admin parameter is not an authorized administrator.

User Action

Verify that the ID specified is an authorized administrator.

DIR0006 The password for the administrator is not valid.

Explanation

The password specified for the administrator is not valid.

User Action

Specify a valid administrator password in the password parameter.

DIR0007 Port %1 is not valid.

Explanation

The port specified is not valid. Valid port numbers are 1 through 65535.

User Action

Specify a valid port in the port parameter.

DIR0008 File %1 is not valid.

Explanation

The session file specified cannot be found or is not valid.

User Action

Verify that the session file can be found in the specified directory, and that it is a valid session configuration file.

DIR0009 %1 is not a valid attribute for the %2 element.

Explanation

The attribute specified is not valid for the element.

User Action

Refer to the online help to determine what attributes may be used with the element.

DIR0010 Attribute not found in %1 element.

Explanation

The specified element requires an attribute.

User Action

Refer to the online help to determine what attributes may be used, and add appropriate attributesS to the element tag.

DIR0011 %1 element not found in document.

Explanation

A required element is missing.

User Action

Refer to the online help to determine what sub-elements are required for the specified element. Specify the missing sub-element within the element tag.

The parser is case sensitive so all elements should be in lower case text or they will not be recognized.

DIR0012 A user, group, or session element must be specified within the %1 tag.

Explanation

A user, group, or session element is a required sub-element for the specified element.

User Action

Specify one of the required sub-elements within the element tag.

The parser is case sensitive so all elements should be in lower case text or they will not be recognized.

DIR0013 A user or group element must be specified within the %1 tag.

Explanation

A user or group element is a required sub-element for the specified element.

User Action

Specify one of the required sub-elements within the element tag.

The parser is case sensitive so all elements should be in lower case text or they will not be recognized.

DIR0014 The %1 group is not valid or does not exist in the directory.

Explanation

The specified group cannot be found or is not valid.

User Action

Specify a valid group identifier or a group which exists in the directory.

DIR0015 A %1 element must be specified for the user.

Explanation

A group must be specified for the user.

User Action

Specify a valid group identifier element for the user. Check the online help for the correct syntax.

The parser is case sensitive so all elements should be in lower case text or they will not be recognized.

DIR0016 The userid is not valid.

Explanation

A valid identifier must be specified for the user.

User Action

The valid characters for a user identifier are English A-Z, a-z, 0-9, . (period), and - (hyphen). When using LDAP, User IDs can be mixed case. When using Host On-Demand to store configuration information, User IDs are converted to lowercase characters. IDs must be unique. You cannot have a user ID and a group ID that are the same, even if one is in lower case and the other is in upper case.

DIR0017 The group is not valid.

Explanation

A valid identifier must be specified for the group.

User Action

The valid characters for a group identifier are English A-Z, a-z, 0-9, . (period), and - (hyphen). The first character must be a letter. When using LDAP, Group IDs can be in mixed case. When using Host On-Demand to store configuration information, Group IDs are converted to uppercase characters.

DIR0018 The %1 element must exist and contain a value.

Explanation

A required element does not exist or does not contain a value.

User Action

Check the online help for the required elements, and specify a value for the required element.

The parser is case sensitive so all elements should be in lower case text or they will not be recognized.

DIR0019 Attribute %1 is only valid when using LDAP. User added without authentication.

Explanation

This is a warning message to let you know that the user has been added without authentication because you have specified native authentication for the user and you are not using LDAP. Native authentication is only available with LDAP.

User Action

If you would like to use native authentication, verify that the Service Manager is configured for LDAP. If you want the user to have authentication and you do not want to use LDAP, update the user to have password authentication.

DIR0020 User added without authentication.

Explanation

This is a warning message to let you know that the user has been added without authentication. The type attribute has a value that is not recognized.

User Action

Check the online documentation for the valid type values for the authentication element, and update the user to have the desired authentication.

DIR0021 Multiple %1 elements are not valid when using LDAP.

Explanation

Multiple groups cannot be specified when using LDAP.

User Action

Choose one group to add the user to and remove the other group elements.

DIR0022 An exception occurred while processing the file import %1.

Explanation

A problem was encountered when importing the specified session file.

User Action

Verify that the session file can be found and that it is a valid session file which can be imported.

DIR0023 The user %1 cannot be found in the directory.

Explanation

The user does not exist in the directory.

User Action

Change the user identifier so that it specifies a valid user ID which exists in the directory.

DIR0024 The group %1 cannot be found in the directory.

Explanation

The group does not exist in the directory.

User Action

Change the group identifier so that it specifies a valid group ID which exists in the directory.

DIR0025 The session %1 cannot be found.

Explanation

The session does not exist for the user or group so it cannot be deleted.

User Action

Change the session identifier so that it specifies a valid session that exists for the user or group. If you added sessions with the same description, the session description will have a number and colon before the it (for example, 1:3270 Display). In order for the session to be deleted the session must have the exact description "1:3270 Display" although the session may have been added with a description of "3270 Display".

DIR0026 %1 not found in the directory.

Explanation

The session cannot be deleted because the user or group does not exist in the directory.

User Action

Change the user or group identifier so that it specifies a valid user or group that contains the session to be deleted.

DIR0027 The %1 element must be specified within the %2 tag.

Explanation

A required element is missing.

User Action

Add the required element within the specified tag.

The parser is case sensitive so all elements should be in lower case text or they will not be recognized.

DIR0028 The %1 group cannot be deleted.

Explanation

HOD is the default group and cannot be deleted when using the HOD directory services.

User Action

Do not attempt to delete the HOD group.

DIR0029 The %1 element is only valid when using LDAP.

Explanation

The specified element is only valid when using LDAP.

User Action

Verify that the Service Manager is configured for LDAP.

DIR0030 The parent group %1 is not valid.

Explanation

The parent group is not valid.

User Action

Specify a valid parent group.

DIR0031 The parent group %1 does not exist in the directory.

Explanation

The parent group specified does not exist in the directory.

User Action

Specify a valid parent group which exists in the directory.

DIR0032 The group cannot be deleted because it contains users or subgroups.

Explanation

When using LDAP, all users and subgroups must be deleted before a group can be deleted.

User Action

Delete all the users and subgroups.

DIR0033 %1 or %2 element must be specified.

Explanation

A groupid or userid must be specified to add or delete a session.

User Action

Specify the userid or groupid within the session tag.

DIR0034 Both %1 and %2 elements may not be specified within the %3 element.

Explanation

Although multiple users or multiple groups may be specified when adding a session, both user and group elements may not be specified at the same time.

User Action

Specify either groups or users when adding a session.

DIR0035 Directory Exception: %1

Explanation

A directory exception was received from the HOD service manager.

User Action

Verify that you have specified the correct administrator ID and password. If the error occurred while processing a user, group, or session, verify that the IDs are valid and exist or do not exist, whichever is appropriate for the action type. Refer to the online documentation for the required elements. Also, verify that the HOD service manager is running.

DIR0036 Parsing Exception: %1

Explanation

The specified error was received when parsing the XML document.

User Action

Correct the error in the document, and run the DirUtil application again.

DIR0037 Exception: %1

Explanation

The specified exception was received.

User Action

Correct the error in the document, and run the DirUtil application again.

DIR0038 Parser Warning: %1

Explanation

A warning was received from the parser.

User Action

Correct the condition which caused the warning, and run the DirUtil application again.

DIR0039 Parser Error: %1

Explanation

An error was received from the parser.

User Action

Correct the condition which caused the error, and run the DirUtil application again.

DIR0040 Parser Fatal Error: %1

Explanation

A fatal error was received from the parser.

User Action

Correct the condition which caused the fatal error, and run the DirUtil application again.

DIR0041 Syntax Error

Explanation

A syntax error occurred when parsing the document.

User Action

Refer to the online documentation for the correct syntax.

DIR0042 %1 is not a valid command.

Explanation

The command is not valid.

User Action

Refer to the online documentation for valid commands.

Java Troubleshooting Checklist

The following are known Java problems with Host On-Demand:

1. [LDAP on AIX with JDK 1.1.8](#)
2. [Exceptions in Java console after screen refresh in Netscape 6](#)
3. [Problem with the Linux Macro Manager under Netscape 6.01, IBM JRE, and Red Hat Linux 6.0](#)
4. [CLASSPATH conflict with WebSphere Studio Application Developer - Integrated Edition](#)
5. [Cannot print some characters on Windows Simplified Chinese platform with Java 2 runtime environment](#)
6. [Simplified Chinese characters display incorrectly under Sun Java plug-in version 1.4 on Red Flag Linux 3.0](#)
7. [Simplified Chinese characters display incorrectly under Windows 2000 Java 2 runtime environment](#)
8. [Users cannot enter user ID or password on client login panel using Netscape 6.21 and Sun JRE 1.3.1.02](#)
9. [Cached administration client problem with Java 2 Plug-in](#)
10. [Can't select saved file list when using file transfer under Netscape 4.x in Red Flag Linux 3.0](#) (opens a different file)
11. [Duplicate warning message when no printer is defined on Windows](#) (opens a different file)

LDAP on AIX with JDK 1.1.8

If you run JDK 1.1.8 on AIX and use an LDAP Directory to store Host On-Demand configuration data, you need to disable a JIT optimization that can prevent the Host On-Demand Service Manager from using LDAP. To disable the JIT optimization, set the following environment variables:

- `export JIITC_SKIPSUBOPT=NBCOPT`
- `export JIITC_SKIPCBNAME=com/ibm/managed/resource/ldap/LDAPResAttrUtils`
- `export JIITC_SKIPMBNAME=constrainResourceAttribute`

Exceptions in Java console after screen refresh in Netscape 6

When you load an enabled session by refreshing the browser screen or using Action > Refresh in Netscape 6, you will find the following exceptions in the Java console. You can ignore the exceptions.

Exception occurred during event dispatching:

```
java.lang.NullPointerException: null pData
```

```
at sun.awt.windows.WInputMethod.handleNativeIMEEvent(Native Method)
at sun.awt.windows.WInputMethod.dispatchEvent(Unknown Source)
at sun.awt.im.InputContext.dispatchEvent(Unknown Source)
at sun.awt.im.InputMethodContext.dispatchEvent(Unknown Source)
at java.awt.Component.dispatchEventImpl(Unknown Source)
at java.awt.Container.dispatchEventImpl(Unknown Source)
at java.awt.Component.dispatchEvent(Unknown Source)
at java.awt.EventQueue.dispatchEvent(Unknown Source)
at java.awt.EventQueue.dispatchEvent(Unknown Source)
at java.awt.EventQueue.dispatchEvent(Unknown Source)
at java.awt.EventQueue.dispatchEvent(Unknown Source)
```


at java.awt.EventQueue.run(Unknown Source)

Problem with the Linux Macro Manager under Netscape 6.01, IBM JRE, and Red Hat Linux 6.0

This problem occurs under Red Hat Linux and Netscape 6 (or later) with the IBM Java runtime environment (JRE) or the IBM JDK for Linux, Service Release 8 and below. When an empty pull-down menu or choice list is clicked (that is, when the leftmost object on the MacroManager Toolbar has no macros present to choose from), the browser, HOD session, and the Linux X-windowing system become unresponsive.

This problem can be avoided by not clicking on the empty pull-down menu, or clicking on the pull-down menu only when there is at least one item to select. However, if the Linux X-window system becomes unresponsive after clicking on the empty pull-down menu, restarting the X-window system returns control back to normal (without having to reboot the entire machine).

To fix this problem, upgrade to the IBM Linux JDK, Service Release 9 or above. This upgrade can be downloaded from IBM DeveloperWorks at <http://www-106.ibm.com/developerworks/java/jdk/index.html>. (New users need to register before downloading it.)

CLASSPATH conflict with WebSphere Studio Application Developer - Integrated Edition

During the installation of WebSphere Studio Application Developer - Integrated Edition (WSAD-IE) (formerly VisualAge(R) for Java), WSAD-IE sets the global environment's CLASSPATH to include the Host On-Demand J2EE connector. This connector has a version of the Host On-Demand code that is common to the Host On-Demand clients. In Netscape 4.x and Internet Explorer 5.x, the browser always loads Java classes from the system CLASSPATH before the network. This means that when WSAD-IE is installed, the browser loads some classes from the connector before loading the correct version of the class from the network.

During WSAD-IE installation, the Windows CLASSPATH is updated to include the following directories:

```
x:\IBM Connectors\class
x:\IBMVJava\eab\runtime30
```

These directories contain .jar files with classes that conflict with Host On-Demand classes. Most users do not need these directories in the classpath because they are used only for Java applications that use WSAD-IE's Host On-Demand connectors.

If Host On-Demand does not work after you install WSAD-IE, try the following workarounds:

- Remove the WSAD-IE entries from the Windows CLASSPATH if you are not developing applications with the Host On-Demand connectors.
- Change the browser to Netscape if the problem is occurring under Internet Explorer.
- Use a batch file to set the CLASSPATH for a specific DOS window to eliminate IBM Connector classes, then launch Internet Explorer (iexplore.exe) or Netscape (netscape.exe) from that DOS window to access Host On-Demand.

Cannot print some characters on Windows Simplified Chinese platform with Java 2 runtime environment

On the Windows Simplified Chinese platform (GB18030 locale) under the Sun Java 2 runtime environment, some characters (including the Euro and the SAA characters) cannot be printed using the Print Screen command. To print these characters correctly, install the IBM Java 2 runtime environment (version 1.3.0-13a).

Simplified Chinese characters display incorrectly under Sun Java plug-in version 1.4 on Red Flag Linux 3.0

Host On-Demand cannot correctly display double-byte characters under the Sun Java plug-in version 1.4 for Red Flag Linux 3.0 (locale: Simplified Chinese) because the Java plug-in does not support the correct font properties file (font.properties.zh). Host On-Demand can correctly display double-byte character set fonts under TurboLinux 6.0 and higher.

Simplified Chinese characters display incorrectly under Windows 2000 Java 2 runtime environment

On the Windows 2000 Simplified Chinese platform, double-byte characters are displayed as square symbols in Netscape 6 and Internet Explorer 6. To display these characters correctly, install the Sun 1.4 Java plug-in or the IBM 1.3.1 Java plug-in.

Users cannot enter user ID or password on client login panel using Netscape 6.21 and Sun JRE 1.3.1.02

Users may not be able to enter user IDs and passwords on the login panel of the Host On-Demand client due to a JRE bug. To avoid this problem, either use the IBM JRE version 1.3 plug-in or click out of the field and onto the desktop and then back into the field.

Cached administration client problem with Java 2 Plug-in

Using the cached administration client with Start Session enabled, you may encounter a gray screen when clicking on the Users/Groups task. If this occurs, please upgrade your Java 2 plug-in to the latest service level.

zSeries Troubleshooting Checklist



If you are experiencing problems with your Host On-Demand installation on the zSeries platform, check the following:

1. Review the steps in the Program Directory. Check the Host On-Demand Web site, <http://www-4.ibm.com/software/webserver/hostondemand/>, as the Program Directory is periodically updated on the Web site.



For more troubleshooting information, check the "Hints and Tips" section of the Program Directory.

2. For SMP/E installs, make sure that the base product was installed first, then verify that the appropriate `hod70mvs.sh` script was executed to move and create the directories before the CSD or PTF was installed. Completely install the base product into UNIX System Services via the `hod70mvs.sh` script, then apply the PTF via the `hod70ptf.sh` script.
3. Use the appropriate shell script to install CSDs and ISB (Interim Service Builds). Use `hod70ptf.sh` for CSD installation according to the ++HOLD information in the PTF associated with the CSD. Use `hodxxmvs.aupsh` to install the ISBs. Follow the instructions provided with the CSD and ISB found on the service key website.
4. If you have just applied a PTF, review the ++HOLD information for the PTF.
5. Check the shell scripts to make sure there are no quotations (") on any of the path statements.
6. To check the level of Java, issue the following command:

```
java -full version
```

Verify the version with the information in the Program Directory.

7. Verify that the PATH and LIBPATH environment variables have been modified for Java. To verify, enter the following commands:

```
echo 'PATH= '$PATH
echo 'LIBPATH= '$LIBPATH
```

If you are using Java 1.1.8, also verify that the CLASSPATH variable is set.

8. Check the NCoDServices.RAS.txt file for errors with the Service Manager. This file can be found in the /private directory. IBM Support may ask for a service manager trace which can be started, stoped and viewed via the Host On-Demand Administrator function under the Services option. See the [Service Manager Trace](#) help for more information. This will record additional debug information in the NCoDServices.RAS.txt file. The file is located in the ...\\hod\\hostondemand\\private directory. The file is recreated with each start of Host On-Demand. It is an ascii file and must be ftp'ed in binary mode to an ascii machine when you are sending it to IBM Support.
9. If the problem occurs during the start of the Service Manager, edit the ServiceManager.sh file to change the java command being executed. Add a # in front of the java command being executed and remove the # for the java command after the comment "This line is for problem determination and outputs to HOD.stdout in the ...\\HOD\\private\\ directory." Save a copy of the NCoDServices.RAS.txt, HODstd, STDERR and STDOUT files.
10. Check the STDERR and STDOUT files if you experience problems when starting or while running the Service Manager.
11. Customized files from the Deployment Wizard must be uploaded to the host in binary mode to the correct directories with the correct permission bits and correct extensions. Use the [DWUnzip](#) utility to set up these files. If you have problems with the utility, you can try to move the files manually:
 1. Set the transfer mode to binary and transfer the files to the host.
 2. Put all .html files in the publish directory (../hostondemand/HOD) or the [alternate read/write publish directory](#) with .ascii appended to the name.
 3. Create a subdirectory .../HOD/HODData (if it does not already exist) with permission bits of 755.
 4. Create a subdirectory .../HOD/HODData/htmlname with permission bits of 755
 5. Put all remaining files in the htmlname subdirectory with permission bits of 755.

6. All files named *.txt must be appended with .ascii.

12. The IBM Support Team may request a copy of the private directory. You can use the pax command to compress all the contents of the private directory. First, cd into the /private directory then issue the following command:

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

The resulting file can then be sent to the Support Team.

13. When upgrading from Host On-Demand version 5 or 6 to version 7, remember to modify the httpd.conf file to change the Pass directives for the .props, .properties and .js files. The names must be changed to include the .ascii extension. If these Pass rules are not changed, the clients will not download because the files cannot be found.
14. If you are concerned about the OS/400 Proxy server port being opened on the OS/390 Service Manager, it can be disabled in the Host On-Demand Administrator by selecting OS/400 Proxy Server in the left frame of the Administrator, then select the No radio button. Then click Apply. The Service Manager will need to be recycled to reflect the change. Port 3470 will no longer be opened.
15. See the [Configuring Host On-Demand on zSeries](#) section in the *Planning, Installing and Configuring Host On-Demand* guide for help with installing and configuring the Host On-Demand configuration servlet and setting up separate read/write private and publish directories on the zSeries platform.
16. If you are experiencing printing problems on zSeries, see [zSeries printing problems checklist](#).

iSeries Problems



If you are experiencing problems with your Host On-Demand installation on the iSeries platform, check the following:

- If you are installing the product for the first time, read the following sections in the *Planning, Installing and Configuring Host On-Demand* guide:
 - [iSeries requirements](#)
 - [Installing on iSeries](#)
 - [Configuring Host On-Demand on iSeries](#)
- If you are installing Host On-Demand on a system where Host On-Demand already exists, verify that you have stopped the Host On-Demand Service Manager prior to installing a new version of the software. Use the ENDHODSVM command to stop the Service Manager.
- After the installation process is complete, check to see if the Service Manager is running. At the command line:
 1. Enter the WRKACTJOB command.
 2. Look for the QSYSWRK SUBSYSTEM:
 - Job QHODSVM should be in TIMW state
 - Job QJVACMDSVR should be in JVAW state
- Is the Java level OK? Run the command DSPDTAARA QJAVA/SF9906x, where x is the last digit of the Java Group PTF in the table below:

OS/400 level	Java Group PTF	JVM 1.3 PTF
V4R4	SF99067	SF63322
V4R5	SF99068	SF63319
V5R1	SF99069	*

* = included with base CD set for OS/400

As new JVM levels are announced, they will become available via PTFs; see <http://www.as400service.ibm.com>. You may also want to obtain the latest Java group PTF and cumulative service.

- Check the job log for QHODSVM for error messages.
- Is the Start job OK? At the command line:
 1. Enter GO HOD
 2. Select option 1
 - If no DATA - Enter the command DLTDTAARA QUSRSYS/QHODCFGD, then select option 1 again.
 - If the start job is still blank, repeat these steps.
- Is the Web server configured properly?
 1. Verify that the http server is running
 2. Stop the Web server using the following command:

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

Note that this command assumes that you are using the default instance of the IBM HTTP server. If you created an instance other than the default supplied by IBM, substitute the name of the instance created for Host On-Demand in this command. For example, if you created an instance called HODWEBSVR, enter the following to stop the instance:

```
ENDTCPSVR *HTTP HTTPSVR (HODWEBSVR)
```

3. Configure the Web server using the following command:

```
WRKHTTPCFG
```

Make sure that active Enable POST and Enable GET entries exist and are not commented out. Add the following entry (there must be one space before the first slash (/) and after the first asterisk (*)):

```
pass /hod/* /QIBM/ProdData/hostondemand/HOD/*
```

This entry creates an alias, hod, for the path to the Host On-Demand files. You must type it exactly as you typed the original directory names, matching upper and lower case.

Press F3 to exit the WRKHTTPCFG tool.

4. Start the Web server using the following command:

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

- If you are experiencing printing problems on iSeries, see [iSeries printing problems checklist](#).
- For more iSeries hints and tips, see the *IBM Host Access Client Package* redbook, available at <http://www.redbooks.ibm.com/redbooks/SG246182.html>.

Deployment Wizard Troubleshooting Checklist

- [General Deployment Wizard troubleshooting](#)
- [Deployment Wizard limitations under Netscape 6.1](#)

General Deployment Wizard troubleshooting

If you are experiencing problems with the Deployment Wizard, check the following:

1. Check the `HODWIZARD.LOG` for error messages that the Deployment Wizard may have written as you created your files.
2. Check that there is enough space to write files on the workstation where the Deployment Wizard is running. Refer to your operating system documentation for information regarding disk space.
3. Check that the `*.html` files you created are in the Host On-Demand publish directory (or an [alternate read/write publish directory](#)) with the other default `*.html` files.
4. Check that the `HODData` subdirectory is correctly installed on the Web server. For example, if you created a Deployment Wizard HTML file called `MyEmulator*.html` there should also be a `MyEmulator*.html` in the publish directory, along with a `\HODData\MyEmulator\` directory with all the Deployment Wizard files.
5. For zSeries, make sure that `*.html` and `*.txt` files have `.ascii` appended to the file name and that the files are transferred to the server in binary format.
6. Check that the permission bits are correctly set on the server for the `HODData` directory, subdirectories, and files. The permissions should be read, write and execute. On zSeries you can set this by issuing the command `chmod 755`.
7. Use the Deployment Wizard to edit the files again to verify that the values you set for your selections were saved correctly. If any values are incorrect, correct them and save your files, then replace the files on the Host On-Demand server by using the [DWUnzip](#) utility.

Deployment Wizard limitations under Netscape 6.1

If your clients use Netscape 6.1 and you are creating customized pages using the Deployment Wizard, you should select a value of **Small**, **Medium**, or **Large** in the **Applet Size** field of the Display tab of the Advanced Options panel. The default value of **Autosize to browser** does not work.

Redirector Troubleshooting Checklist



If you are experiencing problems with the Redirector, check the following:

1. Verify that the inbound IP address and ports defined for the Redirector path are correctly defined as the destination in the client configuration.
2. Verify that the outbound IP address and port defined for the Redirector path is the correct IP address and port of the Telnet Server.
3. Test both ends of the Redirector connection:
 - a. On a Host On-Demand client workstation, ping the Redirector IP address and hostname to verify that the workstation TCP/IP configuration is working. For example, if the Redirector workstation has an IP address of 255.123.123.3, type `ping 255.123.123.3`. If the work station has a host name of `redirecotrws`, type `ping redirecotrws`.
 - b. On the Redirector workstation, ping Host On-Demand client IP address and hostname to verify the server TCP/IP configuration is working.
 - c. On the Redirector workstation, ping TN3270 Server machine, by IP address and host name to verify the server TCP/IP configuration is working.
 - d. On the TN3270E server machine, ping the Host On-Demand Redirector by IP address to verify that the TCP/IP connection is working from the server end.
 - e. Use `nslookup`.
 - f. Make appropriate changes to the server, the client or the Redirector based on the results you receive.
4. Type `Netstat -a` at a command prompt on the Redirector workstation to see if the ports are active.
5. Type `Netstat -a` at a command prompt on the Telnet server to see if the ports are active.
6. On the client workstation, use Telnet to see if the ports defined on the Redirector are accessible through the firewall and network from the client workstation. Consult your firewall documentation for more information. For example, on Windows NT:
 - a. Click Start > Run on the client workstation.
 - b. Type `telnet` and click OK.
 - c. Click Connect > Remote system on the Telnet window menu bar.
 - d. Type the host name of the Redirector in the Host Name field on the Connect window.
 - e. Type the Redirector port (as defined in the Host On-Demand Session properties on the client) in the Port field on the Connect window.
 - f. Accept the default TermType.
 - g. Click Connect.

Consult your operating system documentation for instructions on how to run Telnet on other platforms.

If you receive no messages, the port is open. If you receive "Connect failed with 'Host name,'" then the port is not active. Remember to disconnect after you test each port by selecting Connect > Disconnect from the Telnet window menu.

7. On the Redirector workstation, use Telnet to see if the ports defined on the Telnet Server or other Redirector in series are accessible through the firewall and network. For example, on Windows NT:
 - a. Click Start > Run on the Redirector workstation.
 - b. Type `telnet` and click OK.
 - c. Click Connect > Remote system on the Telnet window menu bar.
 - d. Type the host name of the Telnet server or other Redirector host and the port you want to connect to in the Host Name field and Port field on the Connect window.
 - e. Accept the default TermType.
 - f. Click Connect.

Consult your operating system documentation for instructions on how to run Telnet on other platforms.

If you receive no messages, the port is open. If you receive "Connect failed with 'Host name,'" then the port is not active. Remember to disconnect after you test each port by selecting Connect > Disconnect from the Telnet window menu.

8. Check to see if the Redirector task is active by logging on as the Host On-Demand administrator through `HODMain.html` and using `HODADMIN`.
9. Check to see if the Redirector is listening on the defined port by using the `netstat` command for your operating system.
10. Check to see if the Service Manager is active. If the service manager is not active, the Redirector task will not be active. Use the `netstat` command to see if the Service Manager is active. If the Service manger is not active, start it.

11. Check for messages issued on the Client, especially COMM messages in the emulator [OIA](#).
12. Check for messages on the Telnet Server. Refer to your Telnet server documentation for more information regarding Telnet error messages.
13. If you are using SSL on the Redirector under Windows or AIX with a self-signed certificate, verify that the Host On-Demand Server Key and the CustomizedCAs.class have been created. Note that with a public authority, you do not need to create the CustomizedCAs.class file.
 - a. To create the HOD Server Key:
 - i. If any existing HODServerKeyDb.kdb or CustomizedCAs.class files exist, back them up to a different directory or delete them.
 - ii. Use Certificate Management to create a new CMS key database file (i.e. HODServerKeyDb.kdb). Enter a password for the key database. Make sure that you select to store the password to a file.
 - iii. Select Personal Certificates from the drop-down and create a New Self-Signed Certificate.
 - iv. Extract Certificate as a Base64 .arm file or binary .br file to /hostondemand/bin.
 - v. Save the file to HODServerKeyDB.kdb in the \hostondemand\bin directory.
 - b. To create the CustomizedCAs.class file
 - i. Select Key Database File -> New. Create an SSLight key database class (i.e. CustomizedCAs.class in /hostondemand/HOD). Select Signer Certificates from drop-down and add the .arm certificate file. Label the certificate appropriately.
 - ii. Select Key Database File and Save As and select CMS key database file as SSLight key database. Replace the old file if it exists.
 - iii. Restart the Host On-Demand Service Manager.
 - iv. Modify or create a Redirector service with client-side security.
 - v. Modify or create a session to connect to the above configured redirector with SSL enabled.
 - vi. Prior to connecting at the client, delete the temporary cache prior to starting the session and re-start the browser.
14. It is possible to bypass some potential Java problems that can occur when running Host On-Demand Redirector by passing some additional paramters to Java.
 - a. If you are running the Redirector on the AIX platform, in the NCServiceManager-AIX.sh file, comment out the (#) default Java command and use the following Java command instead:

```
#####
# If running on AIX 4.3 and expect more than 1000 connections, use the
# following invocation
#####
# ulimit -f unlimited
# ulimit -d unlimited
# ulimit -s unlimited
# ulimit -m unlimited
# ulimit -n unlimited
java -DSSL_HANDSHAKE_TIMEOUT=8 -ms16M -mx128M -ss1600k -oss1600k
com.ibm.eNetwork.HODUtil.services.admin.NCServiceManager
/usr/opt/hostondemand &
```

- b. If you are running the Redirector on one of the Microsoft Windows platforms, update the JAVA options as follows. Make the following changes directly in the Windows Registry:
 - i. Open a command window and run regedit.
 - ii. Locate the AppParameters key.
 - iii. Add the following parameters to the key before the -classpath parameter. (Make sure that you leave a space before -classpath and the additional parameters.) For example, on a system with one Gigabyte of memory:

```
-Djava.compiler=NONE -Xrs -Xnoccompactgc -ms256M -mx768M HKEY_Local_Machine
system CurrentControlSet services ibmservicemanager
```

where:

```
-Djava.compiler=NONE - Turns off the just-in-time (JIT) Java compiler
```

```
-Xnoccompactgc - Do not compact during garbage collection
```

-Xms<size> - Sets the initial Java heap size. Adjust this value based on the total memory on your machine.

-Xmx<size> - Sets the maximum Java heap size. Adjust this value based on the total memory on your machine.

-Xrs - Reduces the use of operating system signals

iv. Exit Regedit.

v. From the Windows Control Panel, stop and restart the Host On-Demand Service Manager to make the changes active. If the Host On-Demand Service Manager fails to stop, go back and recheck the parameters you have changed.

Security Troubleshooting Checklist



- [Security troubleshooting steps](#)
- [Common security problems](#)

Security troubleshooting steps

If you are not able to establish a TLS or SSL connection to the server, check the following:

1. What kind of certificate are you using?
 - Self-signed
 - CA
CA's name
2. Where is the certificate stored (for example, is it in the server's keyring)?
3. Have you added the certificate to the Host On-Demand server's keyring database? Issue the `keyring` command from a command prompt. The syntax is:

```
keyring x connect server_name:port_number
```

where:

- `x` is a generic class name
- `servername` is the name of the Host On-Demand server.
- `port` is the port the server is listening on. the default is 443.

Press enter at the password prompt. A list of all the certificates in the server's keyring database is displayed.

4. If you have added a certificate, check the validity dates on the certificate to determine if the certificate has expired.
5. If the certificate is still valid, add it to the Host Onrestartserver keyring. Stop and restart the Service Manager.
6. Add the certificate to the client keyring to make it available to the clients.
7. Use the `keyring` utility to verify the correct certificate and validity dates. For example:

```
keyring CustomizedCAs verify
```
8. Use the `keyring` command to connect to the server on the 12173 SSL port. For example:

```
keyring servername:12173
```
9. Configure a TLS or SSL session on the client to connect to a server on an SSL port (such as 12173).
10. Try removing the Host On-Demand cached client, deleting temporary internet files, and try again. Deleting the temporary internet files removes the current CustomizedCA.class.
11. If possible, verify connectivity by trying to connect. (See [Client does not connect](#) for troubleshooting hints.)
12. Verify that the `HODServerKeyDb.*` files are present in the `\hostondemand\bin` directory. This is the key database file that is used by the HOD redirector and it contains certificates from well-known CAs. It also contains the private key and any personal certificates for the server.
13. If you are using a self signed certificate, verify that the `CustomizedCAs.class` is present in the `\hostondemand\HOD` directory. If you are using a self-signed certificate or a certificate issued by an unknown CA, extract the certificate and include it in the `CustomizedCAs.class` file. This file resides on the HOD publish directory so that the clients can get to it. It is downloaded every time the Host On-Demand client is downloaded.
14. If you are experiencing problems with SSL on the Redirector, verify that the Host On-Demand Server Key and the CustomizedCAs class have been created. See [Redirector Troubleshooting Checklist](#) for details.

Common security problems

If you still experience problems with security or certificates after completing the [security troubleshooting steps](#), the following are some problems that other customers have encountered and their solutions.

1. [COMM662 error message](#)
2. [COMM663 error message](#)

3. [COMM666 error message](#)
4. [Editing the registry if drivers load when starting IKEYMAN](#)
5. [Using two smartcard readers in IKEYMAN](#)
6. [Adding a client certificate](#)
7. [Creating self-signed certificates on Smartcards](#)

COMM662 error message

If you receive a COMM662 error message, the signer certificate of the host's site certificate must be added to the CustomizedCAs.class file on the Host On-Demand server. Extract the signer's certificate into a binary file and transfer it to the Host On-Demand server. On the server, start the Certificate Management program, open or create the CustomizedCAs.class in the Host On-Demand directory, and add the signer's certificate to the CustomizedCAs.class.

COMM663 error message

If you receive a COMM663 error, try turning off "Server Authentication" on the Security tab of the session configuration. This option tells the client not to trust a server if the name in the server's certificate does not trust the server's internet address. The certificate on the server may be using a name that does not match its internet name.

If you receive a COMM663 error message while attempting to establish an SSL session with Host On-Demand, try the following:

1. Select Tools > Internet options > Advanced.
2. Scroll down to the security settings and make sure the box for "Check for publishers certificate revocation" is not checked.

COMM666 error message

If you receive a COMM666 error message, check the certificate to see if it has expired.

Editing the registry if drivers load when starting IKEYMAN

When starting IKEYMAN on a Windows 2000 Host On-Demand Server, an error message occurs when loading slbck.dll during startup. A Schlumberger smart card reader must first be installed and then uninstalled. Some Schlumberger entries may remain in the registry. In order to get rid of this message, a user must clear all Schlumberger entries out of the registry, or they must edit a file in Host On-Demand.

Host On-Demand Certificate Management uses the PKCS11 interface to access smartcard functions. This interface is used mostly for creating self-signed certificates in smartcards, or downloading a certificate in a .pfx or .p12 file to a smartcard.

Before the smartcard can be accessed, additional configuration may need to be done. When Host On-Demand is installed, it is programmed to determine if any smartcards are present in the system. Currently the only smartcards that are recognized are the IBM Security Card and the Schlumberger Reflex readers installed with the Cryptoflex Security Kit V3.0c.

IBM Certificate Management reads all its parameters from an initialization file named ikmunit_hod.properties that is stored in the hostondemand\bin directory. If the IBM Security Card is recognized, the following line will appear in the properties file:

```
DEFAULT_CRYPTOGRAPHIC_MODULE=w32pk2ig.dll
```

This tells IBM Certificate Manager to load this dll when smartcard functions are needed.

If no IBM Security Card is detected, but a Schlumberger card is detected, the line will be similar to:

```
DEFAULT_CRYPTOGRAPHIC_MODULE=C:\\Program  
Files\\Schlumberger\\Smart Cards and Terminals\\Common Files\\slbck.dll
```

These are the only security devices that have been tested with IBM Certificate Management. If there is another security device that implements the PKCS11 interface through a dll, the security device can be tested by changing the name and location of the dll in the ikmunit_hod.properties file.

If the security device is ever removed from the system, IBM Certificate Management will report the following error at startup:

Cryptographic token initialization failed.

To prevent this error, remove the DEFAULT_CRYPTOGRAPHIC_MODULE statement from the ikminit_hod.properties file.

Using two smartcard readers in IKEYMAN

Installing more than one smartcard on the same computer may cause Host On-Demand smartcard support to function incorrectly.

For instance, if the IBM Security Card cannot be opened by Host On-Demand Certificate Manager and a Schlumberger smartcard was previously installed on your computer, there may be values left in your registry that may cause the IBM Security Card drivers to function incorrectly.

To remedy this problem, make a backup of your registry and carefully delete any of the following keys that remain after you have uninstalled the Schlumberger card:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\Readers\Schlumberger ...
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Schlumberger ...
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Schlumberger ...
- HKEY_LOCAL_MACHINE\SOFTWARE\Schlumberger ...

Adding a client certificate

When the Host On-Demand client contacts an SSL server that requests a client certificate, such as Communications Server for Windows NT, Communications Server for AIX, or Communications Server for OS/390 in client authentication mode, the Host On-Demand client may invoke the MSCAPI interface to request all available client certificates. MSCAPI will return all registered certificates, whether they are stored completely in the MSCAPI database, or are associated through MSCAPI with some security device, such as a smartcard or thumbprint reader. The list of certificates that are currently registered in a MSCAPI database can be displayed in the following way:

1. Start the Internet Explorer 5.x browser.
2. From the menu bar, choose Tools then Internet Options.
3. Across the top of the Internet Options panel, choose the Content tab.
4. On the Content panel, click the Certificates button.
5. Across the top of the Certificates panel, choose the Personal tab; if it is not already chosen. These are the certificates that will appear in the drop down list on the Host On-Demand session configuration panel and the Server Requesting Certificate panel. If the certificate is not in this list, it cannot be used by Host On-Demand for client authentication.

Any smartcard or security device that is recognized by MSIE can be used by Host On-Demand for client authentication. Certificates are usually obtained by visiting a web page with the MSIE browser, filling out a form on the web page, and then storing the new certificate in either the browser's database or a security device.

An example of this can be seen by loading http://freecerts.entrust.com/webcerts/ag_browser_req.htm into the MSIE browser [1]. Fill out the information requested, press Proceed to Step 2 and then Proceed to Step 3. At the bottom of this page is a drop down list that lets you specify where to put the certificate.

Choosing Microsoft Base Cryptographic Provider 1.0 will put the certificate into the MSCAPI database. No extra hardware will be needed to access it.

Choosing Schlumberger Cryptographic Service Provider or Gemplus GemSAFE Card CSP v1.0 will put the certificate into a smartcard. If you choose this destination, the name of the certificate will appear in the MSIE Certificates panel; just like a certificate that has been put into the MSCAPI database. However, the certificate will only be accessible if you have plugged in the smartcard by which the certificate was downloaded to.

The certificate obtained from freecerts.entrust.com should be used for testing purposes only. After downloading the certificate, go to the MSIE Certificates panel, as shown above, and choose the Trusted Root Certification Authorities tab. Scroll down the list until you find a certificate issued to Entrust PKI Demonstration Certificates. Highlight this certificate and export it to a file. Then add the exported file to the trusted list of your client authenticating SSL server. With this configuration, the SSL server should trust the Entrust certificate if it is returned by the Host On-Demand client. This exercise should only be used for testing purposes, and the Entrust PKI Demonstration Certificate should be removed from any production server.

[1] 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.

Creating self-signed certificates on Smartcards

Host On-Demand Certificate Management uses the PKCS11 interface to access smartcard functions. This interface is used mostly for creating self-signed certificates in smartcards, or downloading a certificate in a .pfx or .p12 file to a smartcard. (Note: The IBM Security Card supports the creation of a self-signed certificate, but not the downloading of an existing certificate in a .pfx or .p12 file.)

Before the smartcard can be accessed, additional configuration may need to be done. When Host On-Demand is installed, it tries to determine if any smartcards are present in the system. Currently the only smartcards that are recognized are the IBM Security Card and the Schlumberger Reflex readers installed with the Cryptoflex Security Kit V3.0c.

IBM Certificate Management reads all its parameters from an initialization file named ikminit_hod.properties that is stored in the hostondemand\bin directory. If the IBM Security Card was recognized, the following line will appear in the properties file:

```
DEFAULT_CRYPTOGRAPHIC_MODULE=w32pk2ig.dll
```

This tells IBM Certificate Manager to load this dll when smartcard functions are needed.

If no IBM Security Card was detected, but a Schlumberger card was, the line will be similar to

```
DEFAULT_CRYPTOGRAPHIC_MODULE=C:\\Program Files\\Schlumberger\\Smart Cards and  
Terminals\\Common Files\\slbck.dll
```

These are the only security devices that have been tested with IBM Certificate Management. If you have another security device that implements the PKCS11 interface through a dll, it can be tested by changing the name and location of the dll in the ikminit_hod.properties file. If the smartcards are ever removed from the system, these lines should be removed from ikminit_hod.properties.

With this configuration, a self-signed certificate can be created in the smartcard with the following steps:

1. Start IBM Certificate Management
2. On the menu bar, select Cryptographic Token
3. On the Cryptographic Token panel, type in the PIN number of the smartcard, and clear the external database and press OK
4. The Cryptographic Token (smartcard) is now open.

Both the IBM Security Card and Schlumberger cards can create self-signed certificates. The Schlumberger card can also have a certificate in a .p12 or .pfx file imported to the card.

If self-signed certificates are created, then the public portion of the certificates must be extracted (not exported) and added to the trusted list of the SSL server that will request the certificate.

If a self-signed certificate is created in the IBM Security Card, it must be registered with MSCAPI. To do this, start the GemSAFE Card Details Tool. It will check the card, see that the certificate in the card has not been registered with MSCAPI, and ask if you want to register it.

In our testing, not all readers supported all operations on all platforms. Here is a table of what readers were tested on which platforms.

	Entrust	Self-signed	Add .p12	Windows 98/NT	Windows 2000
IBM Security Card PCMCIA Reader	X	X		X	
IBM Security Card Serial Reader	X			X	
Schlumberger Reflex 20 Reader	X	X	X	X	X
Schlumberger Reflex 72 Reader	X	X	X	X	
Schlumberger Reflex Lite	X	X	X		X



OS/400 proxy server



When you enable a proxy server, all the data flows through one configured port instead of multiple ports. Using one port reduces the security risk when transferring files through a firewall.

Enable Proxy Server Service

Click Yes to use a proxy server. If No is selected, the Host On-Demand service manager does not start the proxy server service; port 3470 is not opened.

OS/400 Proxy Server Port

The port to be used by the OS/400 Proxy Server. The default port is 3470.

Maximum Connections

The maximum number of connections to be supported by the OS/400 Proxy Server. If left blank, the number of connections is unlimited.

Related topics

- [Configuring an OS/400 proxy server](#)

Client Troubleshooting Checklist



1. [The client does not download.](#)
2. [The client downloads slowly.](#)
3. [The client does not connect.](#)
4. [You receive a LOG0001 message.](#)
5. [Use Telnet or Netstat to determine if a port is accessible.](#)
6. [Screen Customizer interface doesn't work with the emulator client](#)
7. [Overlapping IME keypad and session window \(DBCS\)](#)
8. [ATTN key applet parameter support](#)
9. [classes.zip CLASSPATH entry may cause connection problem](#)
10. [Cached administration client problem with Java 2 Plug-in](#) (opens different file)

The client does not download

If the client does not download, try the following:

1. Use the Remove Cached Client function under Utilities from the `hodmain.html` web page to remove the Cached client or Administrator client, then try to download the client again.
2. Check that the zSeries Web server has been configured correctly for Host On-Demand files. For example, the `*.js` and the `*.jss` files should be defined so that they are served as ASCII on zSeries. Refer to your Web server documentation for information regarding defining files.
3. Check that all the files and directories under the `.../hod/` directory have read, write and execute permissions. For example on zSeries, you can use `CHMOD filename 755` to set the correct permissions on the file `filename`. Also check `/HODDATA/` and its subdirectories for the correct file permissions.
4. Check the client workstation to make sure there is enough space on the workstation disk to store the Download or Cached client. Refer to your operating system documentation for more information.
5. Check the zSeries Web server `InputTimeout`, `OutputTimeout`, `ScriptTimeout` and `PersistTimeout` values. Make sure the values are large enough to allow the client the time necessary to download over the network. We suggest the following timeout values as a starting point for http web servers:
 - `InputTimeout`: 10 minutes
 - `OutputTimeout`: 20 minutes to 60 minutes
 - `ScriptTimeout`: 10 minutes
 - `PersistTimeout`: 10 seconds

You may need to adjust these values based on your experience and network environment. Refer to your zSeries Web server documentation for more information on setting timeout values.

6. Check that port 8999, if you are using the Configuration Server, is open from the client to the Service Manager machine through the network and all the firewalls in between. Refer to your firewall documentation for more information.
7. Check the client browser's [JVM level](#) to see if it is at a supported level listed in the [Planning, Installing, and Configuring Host On-Demand](#) guide or the [readme](#). If the JVM level is not correct, [upgrade](#) to a higher JVM level and try again.
8. Check the Web server logs for any messages issued during the download time period. Refer to your Web server documentation for more information.
9. Use CTRL-F5, or click Refresh while holding down the shift key to force Internet Explorer to reload the page. Click Reload button while holding down the shift key to force Netscape to reload the page.

10. Check proxy server definitions in the browser. Make sure the browser is using a valid proxy server.

For Netscape:

1. Select Edit > Preferences from the main menu.
2. Click Advanced.
3. Click Proxies. Confirm that the information is correct, or edit the information.
4. Click OK when you are finished.

For Internet Explorer:

1. Select Tools > Internet Preferences from the main menu.
2. Click the Connections tab to view connection information.
3. Click LAN Settings. Confirm that the information is correct, or edit the information.
4. Click OK when you are finished.

11. Do you say "Yes" to trust content from International Business Machines when prompted?
12. Check whether a proxy setting is being used in the Internet Explorer LAN settings.
13. Make sure that the browser has Java Scripting turned on and that the firewall does not block Java Scripts. Host On-Demand clients use Java scripting.
14. Check whether a program that disables pop-up messages has been installed on the client machine. Host On-Demand issues pop-up messages, so disabling pop-ups can cause Host On-Demand to stop processing.

Client does not download under Internet Explorer

If you are having difficulty loading a Host On-Demand client under Internet Explorer, follow the steps in this section to resolve the problem.

The following steps do not require you to be connected to the Internet. The purpose of these steps is to reset Internet Explorer to the correct state to allow the Host On-Demand client to load.

1. Clear the browser cache. Do this as follows on the Internet Explorer toolbar: select **Tools**, point to **Internet Options**, then select **Delete files**. Be sure to check "all offline content".
2. In the same **Internet Options** window, select **Settings**, then point to **View objects** and make sure there is no Host On-Demand object installed. These objects would have names such as "Host On-Demand 4.0."
3. In the same **Internet Options** window, select **Content** then point to **Publishers**. Delete **International Business Machines** from the list of trusted publishers
4. In the same **Internet Options** window, select **Advanced**, then select **Restore Defaults**. Click Apply and then OK
5. Enable the Internet Explorer Java Console. In the Same **Internet Options** window select **Advanced**.
 - a. Scroll down to the Microsoft VM section and click on the 3 checkboxes in this section. Select the following 3 options:
 - Java Console Enabled
 - JIT Compiler for Virtual Machine Enabled
 - Java Logging Enabled
 - b. Select Apply
6. Check for the browser proxy settings:
 - a. Choose the **Connections** property page
 - b. If **Use a proxy Server** is checked, record the values set for proxy server on this panel.
 - c. Select **Advanced**.
 - d. On the **Proxy Settings** panel, record the values (if any) for the proxy address being used for each of the proxies listed.
 - e. Select OK.

- f. Select OK.
- g. Select OK.
7. On the Internet Explorer toolbar, select **Help** then select **About Internet Explorer**. What version of IE are you using? Record this information for use later.
8. Exit out of Internet Explorer and select **My Computer** on your desktop

These next steps do not require you to be connected to the Internet unless you decide to download code from Microsoft as described in step 6.

1. Make sure there is sufficient space for the client on your hard drive. 5Mb should be sufficient. You can do this by going to **My Computer** on your desktop and selecting your drive with a right mouse click. Select **File > Properties** to determine how much disk space is available.
2. Use the Remove Cached Client utility from the HODMain.html page, then delete any remaining partially installed files from Host On-Demand version 5 or version 6 clients such as the following:
 - o HODDATA
 - o HODCC
 - o HOD_CCR.*
 - o hodprint.*



Deleting these files removes your user preferences and any recorded macros.

To find out if these files exist on your PC go to the Start menu, select **Search**, select **Files Or Folders**, type the name of the file/folder you want to search for in the **Named** box, select to search all your drives in the **Look In** box, and then click **Find Now**.

3. Go to **Start**, select **Settings** then select **Control Panel**. Click on **Add/Remove** programs and select Internet Explorer. Choose the REPAIR option.
4. Exit out of the control program and back to your normal Desktop.
5. Restart your PC.



This option may not be available if you are using Windows 2000 SP2. Check the Microsoft web site on how to repair Internet Explorer when you are using Windows 2000.

6. You may want to check the Microsoft Web site for the latest Microsoft JVM and, if it is a later version than the one you are currently using, install it.

To display the Java Console and determine the level of JAVA you are currently running, select **View** on the Internet Explorers Toolbar, then point to **Java Console**. The Java Console window appears. The level is the last 4 digits as seen in the first line of the Java console. For example:

```
Microsoft (R) VM for Java, 5.0 Release 5.0.0.3805
```

If you decide to upgrade the code on your machine, download the build from the Microsoft web site and save it on your PC. When the download is complete, close the browser, double click on the downloaded file and follow the instructions for installing the JVM. You need to restart your PC to complete the installation process



Reinstalling the latest JVM sometimes resolves problems if nothing else has worked.

Client does not download under Netscape

These steps do not require you to be connected to the Internet. The purpose of these steps is to reset Netscape Navigator to the correct state to allow the Host On-Demand client to load.

1. Use the Remove Cached Client utility from the HODMain.html page, then delete any remaining partially installed files from Host On-Demand version 5 or version 6 clients such as the following:
 - o HODDATA

- HODCC
- HOD_CCR.*
- hodprint.*



Deleting these files removes your user preferences and any recorded macros.

To find out if these files exist on your PC, select each of your listed hard drives under **My Computer**. Right mouse click on the drive and select **Search**. Now search for each of the files/folders listed above. When you find one of these files, delete it.

2. Exit out of **My Computer** and back to the Desktop.
3. Try doing a shift+F9 or Shift+Refresh after loading the client.
4. Delete temporary Internet files. Choose **Edit** from the toolbar, select **Preferences**, select **Advanced**, then select **Clear Disk Cache**.
5. Record any proxy settings you have configured the browser with. To do this choose **Edit** from the toolbar, select **Preferences**, then select **Advanced**. Point to **Proxies** and record any proxy settings on this panel. If **Manual proxy configurations** is selected then choose **View**. Record all the values you have configured on this page.

The client downloads slowly

If the client downloads slowly, try the following:

1. Check to see if other network traffic is also slow.
2. Make sure other pages are not also downloading slowly. Try to download a non-Host On-Demand HTML page to see if the problem is a Web server problem. If it is a Web server problem, refer to your Web server documentation for more information.
3. Check to see if port 8999 is active, if you are using the Service Manager to manage user configurations. The client may be trying to connect back to the service manager, using processor resources and therefore slowing any downloads. If the port is not active, activate it. Refer to the server's operating system documentation for more information regarding ports.
4. If this is a dial-up connection, you can use the Host On-Demand Deployment Wizard to create a smaller Download or Cached client with only the features your users need to use.
5. Check the Web server logs for errors.

The client does not connect

If the emulator client applet loads but the emulator session does not connect, try the following:

1. Check for messages in the [OIA area](#) of the session window. For example, look for COMM or MACH messages on the lower left portion of the session window. To see an [explanation of the COMM and MACH messages](#):
 - a. Click Help on the Host On-Demand session menu. The Help system loads in the default system browser.
 - b. Select the Index tab.
 - c. Click **O**. Click **OIA** in the index to display a list of the messages.
 - d. Click on the message you want to see.
2. Make sure the parameters on the Telnet server and client match and fix them if they do not.
 - a. Verify that the host specified in Host On-Demand's configuration is the same as the hostname configured for the TN3270E Server.
 - b. Verify that the port number specified in Host On-Demand's configuration is the same as the port number configured for the TN3270E Server.
3. Make sure that TCP/IP is working on both machines and that all the connections are active by pinging host names and IP address.

- a. On the Host On-Demand client workstation, at a command prompt, ping the client itself by IP address to verify that the workstation TCP/IP configuration is working. For example, if the Host On-Demand client workstation has an IP address of 255.123.123.3, type `ping 255.123.123.3`.
 - b. On the Host On-Demand client workstation, ping the client itself by host name to verify that the workstation TCP/IP and DNS configuration is working. For example, if the Host On-Demand client workstation's hostname is `myclient`, type `ping myclient`.
 - c. On the emulator host server, ping the server itself by IP address to verify that the server TCP/IP configuration is working.
 - d. On the emulator host server, ping the server itself by host name to verify that the server TCP/IP and DNS configuration is working.
 - e. On the Host On-Demand client workstation, ping the TN3270E Server machine by IP address to verify the TCP/IP connection is working.
 - f. On the Host On-Demand client workstation, ping the TN3270E Server machine by host name to verify that the TCP/IP and DNS connection is working.
 - g. On the emulator host server, ping the Host On-Demand client workstation by IP address to verify the TCP/IP connection is working from the server end.
 - h. On the emulator host server, ping the Host On-Demand client workstation by host name to verify the TCP/IP and DNS connection is working.
 - i. On a command line, type `nslookup w.x.y.z`, where `w.x.y.z` is the dotted decimal address of the host. If the client is given a numeric address, it contacts the local DNS to get the host name. Sometimes the DNS is not setup properly for this reverse look-up. If the DNS is not setup properly, add the host name and address to the `HOSTS` file on the client.
 - j. Make appropriate changes to the server, the client or the redirector based on the results you receive.
4. Check that the following ports are open through the network routers and firewalls from the client to the Web server, Service Manager, and Telnet server. Refer to your server operating system and router documentation for more information regarding ports.
 - Web server port 80.
 - Service Manager port 8999.
 - Telnet ports 443, 23, and so forth, as appropriate for the Host On-Demand functions you are using.
 - Look at the [Java Console](#) for error messages.

You receive a LOG0001 message

If you get a Log0001 message, try the following steps. A LOG0001 could be caused by:

1. A problem at the client machine. Check for Java errors or exceptions in the [Java Console](#), TCP/IP errors in the network reaching the Service Manager machine, or caused by a mix of Host On-Demand download/cached clients. Use `HODRemove.html` to remove the Cached client.
2. A problem at the Host On-Demand Service Manager machine. Check for a system abend, looping task, hung tasks, Java abends, check for error messages in `NCoDservices.RAS.TXT`.
3. If there are no messages and the client appears to connect, check to see if all the Web server, Host On-Demand, and Telnet ports are active (especially port 8999).

Use Telnet or Netstat to determine if a port is accessible

To use Telnet or Netstat to determine if a port is accessible, do the following:

1. Type `Netstat -a` at a command line to see if the ports are active. If not, refer to your operating system documentation for information regarding activating ports.
2. Check for messages in Host On_Demand message and trace log `NCoDservices.RAS.txt`, located in the `\private` directory.

3. Check to see if a port on the Service Manager or through the firewall is active. For example, under Windows NT, use Telnet on the Windows client workstation:
 - a. Click Start > Run
 - b. Type `telnet` and click OK.
 - c. Click Connect > Remote system on the Telnet window menu bar.
 - d. Type the host name you want to connect to in the Host Name field on the Connect window.
 - e. Type 8999 (or other ports based on the problem) in the Port field on the Connect window.
 - f. Accept the default TermType.
 - g. Click Connect.

If you receive no messages, the port is open. If you receive "Connect failed with 'Host name,'" then the port is not active. Remember to disconnect after you test each port by selecting Connect > Disconnect from the Telnet window menu.

Refer to your operating system documentation for instructions regarding how to run Telnet on other operating systems.

Screen Customizer interface doesn't work with the emulator client

If you are using an old HTML file from a previous release, the Screen Customizer interface may not come up or a Null Pointer exception message may be displayed when starting a session. If this happens, you may need to edit the html file, and replace any occurrences of `scbase.jar` or `scbase.cab` and `scfull.jar` or `scfull.cab` with `sccbase.jar` or `sccbase.cab`.

Overlapping IME keypad and session window (DBCS)

If the IME keypad overlaps a Host On-Demand session window, you may get incorrect results when you click the mouse in the keypad.

ATTN key applet parameter support

The ATTN key value might not be recognized by some applications. If not, you can use the ATTN key parameter to specify the byte stream sent to the server when the ATTN key is pressed.

The syntax for the ATTN key parameter is:

```
<PARAM Name=attnKeyOverride VALUE=dddd>
```

When a session is connected in basic TN3270 mode, Host On-Demand sends the following commands to the telnet server when the ATTN key is pressed: `PA1`, `IAC`, `EOR`, `IAC`, `BREAK` (in hexadecimal form: `6CFFEFF3`)

`PA1` is the SNA AID key value for the `PA1` key. This ATTN key value is the same default value used by Personal Communications.



- The value dddd is the hexadecimal digits sent to the telnet server when the ATTN key is pressed. For example, if you want the Telnet command `IAC BREAK` sent to the server, then use the following value: `FFF3`.
- The parameter name is case sensitive; the parameter value is not.
- Spaces must not be inserted between the hexadecimal digits, or between the equal sign and either the parameter name or parameter value.
- The hexadecimal value specified must be a valid sequence of one or more telnet commands.
- The ATTN key override value is only applicable if the session is connected in basic TN3270 mode, regardless of the session's TN3270E property setting. If the session is connected in TN3270E mode then the ATTN key value of `FFF4` (IAC, Interrupt Process) is always sent to the telnet server.

classes.zip CLASSPATH entry may cause connection problem

If you are using file transfer on a 5250 emulator session, using the HODCached applet, or loading the Database On-Demand applet and having host connection problems, check to see if you have a classes.zip entry in your CLASSPATH. If so, remove it but be aware that other programs may require this classpath entry.

Printing Troubleshooting Checklist



1. [Serial printing not supported](#)
2. [Spaces between Hindi characters when printing the screen](#)
3. [Print Screen on Windows 2000 in a session using monospaced fonts](#)
4. [Multi-language limitations on "Select Printer" function](#)
5. [Select Printer feature available on Windows clients only](#)
6. [Duplicate warning message when no printer is defined on Windows](#)
7. [Printing problems under Netscape 4.x and Windows](#)
8. [3270 printing problems under Windows platforms or with USB printers](#)
9. [5250 host printing troubleshooting checklist](#)
10. [3270 host printing troubleshooting checklist](#)
11. [Screen Customizer printing troubleshooting checklist](#)
12. [Print screen not available on some Unix platforms](#)
13. [Cannot print some characters on Windows Simplified Chinese platform with Java2 runtime environment \(opens different file\)](#)

Serial printing not supported

Host On-Demand does not support printing to serial printers attached to COMx ports.

Spaces between Hindi characters when printing the screen

When using the print screen facility to print a screen which has composed Hindi characters, you may notice that there are spaces between the composed Hindi characters.

Print Screen on Windows 2000 in a session using monospaced fonts

If your monospaced Host On-Demand session font, such as MS Gothic or MS Mincho, is mapped to one of PAGES' fonts, you must set your Windows 2000 printer driver to Don't Substitute fonts in order to Print Screen. MS Gothic and MS Mincho fonts are mapped to PAGES' Gothic and PAGES' Mincho fonts by default, which results in incorrect print screen output.

Multi-language limitations on "Select Printer" function

When editing the hodmodel.properties and hodpdt.properties files you must enter PDT and model names **exactly** as they appear in the PDT or model field of the Printer tab. The PDT and model fields are translated, so the hodpdt.properties and hodmodel.properties files must be in the same language as the Host On-Demand clients that are trying to use the Select Printer function. There can only be one set of printer selection properties files on a Host On-Demand server, so all the clients using the Select Printer function must be in the same language as the properties files.

Select Printer feature available on Windows clients only

The Select Printer feature is available only on Windows clients. You will not see a Select Printer button on the Printer tab when running Host On-Demand on clients other than Windows.

Duplicate warning message when no printer is defined on Windows

When no printer is defined on Windows and a print screen-related operation (such as Page Setup or Print Setup) is attempted on a Host On-Demand version 7.0 client running with a Java 2-enabled browser, a message appears asking whether the user wants to install a new printer. If "No" is chosen, the same message may appear again. This is a JVM problem; the message is shown by Windows, not by HOD. The workaround is to press the "No" button again.

Printing problems under Netscape 4.x and Windows

If you configure a Host Print session or use the Windows printer function on the Netscape 4.x browser running on a Windows platform, you must turn the Just In Time (JIT) compiler on.

3270 printing problems under Windows platforms or with USB printers

Windows 95, Windows 98, Windows Me, and USB printers

If you are using Windows 95, Windows 98, Windows Me, or a USB printer and are having problems printing, try the following.

- Use Windows Native Printer support. For more information, see [Help for Printing a Screen](#).
- If Windows Native Printer support does not work, write a batch file to redirect the output to the printer.
 1. In the Associated Printer window, right mouse click on the printer icon and select Properties.
 - a. Select the Printer tab.
 - b. Select print to a file.
 - c. Set Print to separate files to Yes.
 - d. On the printer definitions, the Print to file line looks like this:

```
c:\tmp\hodprt.* | c:\tmp\xxx.bat $
```

where \tmp is some folder that exists that you do not mind putting the files in.

2. Make a batch file that contains these commands.
 - a. Open Notepad.
 - b. Copy or type these commands into Notepad.

```
echo off
```



```
copy %1 lpt1
```

```
erase %1
```

```
exit
```

- c. When you are finished select FILE then Save As.
- d. Change the Save as type to be All files
- e. Change the encoding to be ANSI
- f. In the Filename field type in the file name as xxx.bat

Windows NT and Windows 2000

For printing problems under Windows NT or Windows 2000, try redirecting printer output to a folder on your desktop. Do the following:

- Use Windows Native Printer support. For more information, see [Help for Printing a Screen](#).
 - If Windows Native Printer support does not work, write a batch file to redirect the output to the printer.
1. In the Associated Printer window, right mouse click on the printer icon and select Properties.
 - a. Select the Printer tab.
 - b. Select print to a file.
 - c. Set Print to separate files to Yes.
 - d. On the printer definitions, the Print to file line looks like this:

```
c:\hodprnt\hodprt.* | c:\tmp\xxx.bat $
```

where \tmp is some folder that exists that you do not mind putting the files in.

2. Make a batch file that contains these commands.
 - a. Open Notepad.
 - b. Copy or type these commands into Notepad.

```
echo off
```

```
copy %1 lpt1
```

```
erase %1
```

```
exit
```

- c. When you are finished select FILE then Save As.
 - d. Change the Save as type to be All files
 - e. Change the encoding to be ANSI
 - f. In the Filename field type in the file name as xxx.bat
3. Use Windows Explorer to create a folder called c:\hodprnt.
4. Add a shortcut on your desktop that points at the c:\hodprnt folder on your hard drive.
5. When you print, double click on the shortcut. This opens the folder on your hard drive with the hod print files.
6. Double click on the file you want to print, open the file in Word, Notepad, WordPad, or your favorite text editor, then print the file.

5250 host printing troubleshooting checklist



Host On-Demand uses Host Print Transforms.

If you cannot print correctly, try the following:

- If you are receiving printouts that are blank or have "garbage" characters, make sure that the model and manufacturer of the printer match the printer defined in the Host On-Demand printer session and the iSeries system. To check the model and manufacturer on the AS/400, do the following:
 1. Enter the following command from the command line using a 5250 display session with the printer session started


```
Wrkcfgsts *dev qpa
```


or


```
Wrkcfgsts session_name
```
 2. Choose OPT 8 = Work with device.
 3. Select the QPA or session that you are working with.
 4. Choose Opt 5 = Display and press enter.
 5. Page down and on the 9th line you will see the manufacturer and model of the printer.
- If the manufacturer type and model of the printer defined on the AS/400 and the Host On-Demand session match, check with the manufacturer to determine which drivers work with the list that Host On-Demand provides.
- You may want to have a Host On-Demand level 3 transport trace and a copy of the printout printed to a file in case you plan to contact IBM.

3270 host print troubleshooting checklist

Things to check if you are not printing correctly using TN3270:

- You may want to try upgrading your JVM level.
- Try printing from another browser.
- If you are using LUs in the configuration of Host On-Demand, check to see you have TN3270E.
- If you are printing using the native windows printing as the default, use Other and explicitly select the printer.
- If you are using a printer definition table (PDT), make sure that you are using the correct PDT for the brand of printer that you are trying to print to.
- Try printing to a file rather than directly to the printer. Then, open the file in a application that you can print from to see if the printout is different from the original printout.
- If you are using Screen Customizer, try printing without Screen Customizer enabled.
- If you have a networked attached printer, check to see if you can connect the printer or a printer locally to your PC and print. See if there is a difference with the printout from the original printout.
- You may want to have a Host On-Demand level 3 transport trace and a copy of the printout printed to a file in case you plan to contact IBM.

Screen Customizer printing troubleshooting checklist

MERGE WITH givetoservice checklist

Use the following checklist for contacting customer service if you experience printing problems with Screen Customizer.

- HOD Version
- Telnet server
- Client platforms
- Browser and JVM level
- Local or Networked attached printers
- Are you trying to do a print screen?
- What type of printer are you using? (HP, Lexmark, etc)
- How was the printer session created?
- Has printing worked before now?

Check the following when using Screen Customizer if you are not printing correctly.

- Check to see if you can print without Screen Customizer enabled.
- Upgrade the JVM level to the latest level.
- Try printing from another browser.
- Try setting Parameter "OldPrintScreen value=true".
- Request a transport layer trace, level 3.

Print screen not available on some Unix platforms

The Print Screen function of Host On-Demand uses a programming interface provided by Java. It works on most platforms, but it does not work on some Unix-based operating systems, such as Linux. The implementation of the programming interface uses the Unix lp command, which is not available on some Unix-based operating systems.

Following is the workaround for this problem:

1. Log into the system as a superuser.
2. Open a terminal session to input commands from prompt.
3. Change directory to the directory where lpr command is stored. Typically, it is /usr/bin. If this is so, type

```
cd /usr/bin
```

4. Create a symbolic link with the ln command. Type

```
ln -s lpr lp
```

5. Log out.
6. Log in to the system as a user and start a Host On-Demand display session.
7. Click File > Print Screen.
8. Delete the string specified for Banner Page Title. By default, it is specified like Print Screen.
9. Press OK.

Browser problems



If you are experiencing problems that you suspect may be caused by your browser, see the list of known problems for the browser you are currently using:

- [Internet Explorer problems](#)
- [Netscape problems](#)

Internet Explorer problems

- [Erratic behavior](#)
- [Using remapped Alt-key combinations](#)
- [Print Screen might not work within the Screen Customizer interface](#)
- [Checking and upgrading the JVM level for Microsoft Internet Explorer](#)
- [Online revocation server error](#)

Erratic behavior

If you experience erratic behavior when using Microsoft Internet Explorer 4.0, you can often fix it by disabling the Just-in-Time (JIT) compiler:

1. From the browser's menu bar, click View > Internet Options.
2. Click the Advanced tab.
3. In the Java VM section, clear the Java JIT compiler enabled check box.
4. Close the browser.
5. Reboot your workstation.

Using remapped Alt-key combinations in Internet Explorer

The JVM in Internet Explorer handles key-events differently according to its level. Remapped Alt-key-combination key-events are sometimes sent to the menu even after the action for the remapped key is taken. The result is that focus is put onto the menu and remains there. To regain focus, click on the active screen.

This problem is fixed in JVM levels 3167 and later.

Print Screen might not work within the Screen Customizer interface

On later versions of the Microsoft JVM, including the version that ships with Internet Explorer 5.0, Print Screen within the Screen Customizer Interface might not work.

Checking and upgrading the JVM level for Microsoft Internet Explorer

You must have JVM level 3165 or later installed in order to use Microsoft Internet Explorer with Host On-Demand. To determine what JVM level is currently installed, you can view Internet Explorer's Java console by doing the following:

1. [Enable the Java console](#) display.
2. Select View > Java console

If you need to update the JVM, you can either:

- Download an updated JVM for your installed version of Internet Explorer from Microsoft.

- Install one of the supported levels of Internet Explorer (4.01 with SP1 and 5.x or later), choose Custom Installation during installation and select Update JVM. **Note:** Selecting a Typical Installation of Internet Explorer does not update the level of a pre-installed JVM.

Online revocation server error

When installing the Host On-Demand cached client, Internet Explorer may display a Security Warning and report the following message:

An error occurred while accessing the online revocation server.

This error message occurs when the Certificate Revocation option in Internet Explorer is selected. You will be unable to connect to the server to verify that the certificate has not been revoked. To prevent this message, disable the option by selecting Internet Options > Advanced > Security and unchecking "Check for Publisher's Certificate Revocation".

Netscape problems

- [Loading HOD*.html after HODAdmin.html](#)
- [Error using the User Profile Manager on Netscape browsers with the Locally installed client](#)
- [Repeatedly logging on and off clients using Netscape causes the clients to function improperly](#)
- [AIX Netscape clients crash when running Telnet-negotiated security and Client Authentication](#)
- [Netscape session restrictions on Windows 95 and 98](#)
- [Saving session configuration changes when using UNIX Netscape clients](#)
- [Cached client limitation](#)
- [URL display errors under Netscape 4.x on Chinese-Traditional Windows platforms](#)
- [F10 key doesn't function in Host On-Demand with Netscape on UNIX](#)
- [Can't select saved file list when using file transfer under Netscape 4.x in Red Flag Linux 3.0](#)
- [Macro problems under Netscape 4.x on Linux](#)
- [IME no response problem on Netscape 4.x on Linux](#)
- [Printing problems under Netscape 4.x and Windows](#) (opens a different file)
- [Deployment Wizard limitations under Netscape 6.1](#) (opens a different file)
- [Exceptions in Java console after screen refresh in Netscape 6](#) (opens a different file)
- [Problem with the Linux Macro Manager under Netscape 6.01, IBM JRE, and Red Hat Linux 6.0](#) (opens a different file)
- [Users cannot enter user ID or password on client login panel using Netscape 6.21 and Sun JRE 1.3.1.02](#) (opens a different file)

Loading HOD*.html after HODAdmin.html

When using Netscape, you cannot load any of the client applets after loading HODAdmin.html, or vice versa. To correct this problem, do one of the following:

- Shut down and restart the browser before you load the HOD*.htm.
- While holding the Shift key, click Reload in the browser to load the client file.

Error using the User Profile Manager on Netscape browsers with the Locally installed client

When using the User Profile Manager on Netscape browsers while loading the Locally installed client from the Start menu, you may see the error "Cannot find the file "C:\hostondemand\HOD_en.html" (or one of its components). Make sure the path and filename are correct and that all required libraries are available." Click OK and the Locally installed client will load in the browser.

Repeatedly logging on and off clients using Netscape causes the clients to function improperly

Logging on and off any of the Host On-Demand clients repeatedly without restarting the Netscape browser first can cause the browser to remove files from cache that are needed in order for the clients to function properly. The browser removes files in order to reduce the cache. Restart your browser after logging off and before logging on to any Host On-Demand clients while using Netscape to prevent problems with the clients.

AIX Netscape clients crash when running Telnet-negotiated security and Client Authentication

AIX clients accessed through the Netscape browser crash when running Telnet-negotiated security and client authentication at the same time. You can either configure the clients to use Telnet-negotiated security or to use client authentication, but not both simultaneously.

Netscape session restrictions on Windows 95 and 98

Due to a restriction in the Netscape browser on Windows 95 and 98, you can start a maximum of 10 to 12 Host On-Demand sessions before Netscape runs out of resources.

Saving session configuration changes when using UNIX Netscape clients

When using the Netscape browser on a UNIX client, including Linux and AIX, make sure all the sessions you are using are closed before shutting down the browser, so that the latest changes made to the sessions (screen size and position, colors, etc.) are saved. This is not necessary for clients on operating systems other than UNIX because session configurations are saved to the server before the browser shuts down.

Cached client limitation

If you use Netscape 4.7x with the cached client, avoid using the key combination Shift-Reload to reload the Host On-Demand HTML page. If you use this key combination, the Host On-Demand applet cannot be used and you must restart your browser. Close your browser, restart it, and point it to the Host On-Demand server to continue.

URL display errors under Netscape 4.x on Chinese-Traditional Windows platforms

If you are using Netscape 4.x on a Chinese-Traditional (Taiwan) Windows platform, URLs that are displayed on 3270 and 5250 session screens may be truncated and overlap with text on the same row. A limitation in the Sun Java virtual machine (JVM) version 1.1.5 causes Netscape 4.x to return the wrong character width value for this platform.

To fix this problem, upgrade to Netscape version 6 or later.

F10 key doesn't function in Host On-Demand with Netscape on UNIX

The Unix version of Netscape is built on the Motif toolkit, which binds the F10 key to a command that activates the menu bar by default. As a result, the terminal emulation screen of Host On-Demand running on Unix versions of Netscape cannot handle the F10 keystroke.

There are two workarounds:

1. Use the key remap function of Host On-Demand to remap the F10 key to another key position. This will keep the default key positions for Motif, you must press a different key to send F10 in the Host On-Demand terminal emulation screen.
2. Use the xmodmap or xkeycaps program to swap the F10 key with another key. The X Window system can remap key functions to any physical keys; therefore, you can use it to swap the F10 key to a key that is not frequently used. For information on how to remap the key, refer to the main page of the xmodmap program or the xkeycaps Web page at <http://www.jwz.org/xkeycaps/>.

Can't select saved file list when using file transfer under Netscape 4.x in Red Flag Linux 3.0

When you load a file transfer list under Netscape 4.x in Red Flag Linux 3.0, the list does not display due to a bug in the Sun JVM 1.1.5 of Netscape 4.x. To fix this problem, upgrade to Netscape 6.

Macro problems under Netscape 4.x on Linux

A macro may hang under Netscape 4.x on Linux if the user creates the macro action "Run Program" and selects the option to wait for the program to return before continuing to execute the macro. To fix this problem, upgrade to Netscape 6.

IME no response problem on Netscape 4.x on Linux

Under Netscape 4.x (HotJava JDK 1.1.5) on Linux, the input methods switch (IME) is not working due to a problem with the JDK on the Linux platform. (See <http://developer.java.sun.com/developer/bugParade/bugs/4339460.html> for more information about this JDK problem.) To fix this problem, upgrade to Netscape 6.

Miscellaneous Troubleshooting Issues



The following are some miscellaneous problems that other customers have encountered and their solutions.

- [Starting on Red Hat Linux or zSeries](#)
- ["Unable to initialize threads" message when trying to start HODSRV on OS/390](#)

Starting on Red Hat Linux or zSeries

The message **No such file or directory libjavaskit.so** may appear when Host On-Demand is started on Red Hat Linux or zSeries. The error message is informational and does not affect the functionality of Host On-Demand on Linux or zSeries.

This applies to all platforms other than Window NT and AIX, including Windows 2000, Solaris, and other Linux vendors.

"Unable to initialize threads" message when trying to start HODSRV on OS/390

If you are starting the ServiceManager on OS/390 and you receive an error message that states **Unable to initialize threads: cannot find class java.lang.Thread**, do one of the following:

- Uncomment the following line in the ServiceManager.sh script file:

```
export CLASSPATH==/usr/lpp/java/J1.1/lib/classes.zip
```

- Specify the CLASSPATH and LIBPATH in the /etc/profile file as described in the Host On-Demand Program directory.

The TraceOptions HTML parameter

You can start and control the Host On-Demand trace facility for an emulator session using the `TraceOptions` parameter in an HTML file. As an Administrator, you can send the customized HTML file to a user. You will not have to explain to the user how to set up and start the trace facility before they can capture a trace of the problem.

Host On-Demand servers running on Win32, AIX, Sun Solaris, OS/2, Novell Netware, OS/400, MVS/390 and Linux support the `TraceOptions` parameter. The parameter has been added to the Cached client with problem determination (`HODCachedDebug.html`) and the Download client with problem determination (`HODDebug.html`), but is commented out. If you want to send either of these files to a user so the user can capture a trace, uncomment the `TraceOptions` parameter. You can also add the `TraceOptions` parameter to any custom HTML you have created. Custom HTML files must also include the problem determination components. There is a sample file, `cmptrace.html`, that can show you how to use this parameter. It is located in the `x:\hostondemand\hod\ibmserv` directory. The `TraceOptions` parameter also works with `Session1`, `Session2` and bookmarked sessions that include the problem determination components.

When an HTML file passes the Host On-Demand server the `TraceOptions` parameter, the server:

- Starts the session and tracing with the specified options.
- Displays a window informing the user that a trace has started and also prompts the user to click End Trace to stop the trace and then write it to a file.
- Displays a window informing the user that the trace has been saved when the user clicks End Trace, and prompts the user to click OK to remove the window.

Related topics:

- [Configuring the TraceOptions HTML parameter](#)
- [The IPMonitor HTML parameter](#)
- [IP Monitor](#)
- [Viewing a User's Trace](#)
- [Tracing on the Server](#)
- [Tracing on the Client](#)
- [Log and Trace Messages Format](#)
- [Setting Trace Levels](#)
- [Changing the trace settings \(client\)](#)

Configuring the TraceOptions HTML parameter

You can configure HTML files to trace debugging information by adding the `TraceOptions` parameter to the `APPLET` tag in the HTML file. You can add the `TraceOptions` parameter to session HTML files in two ways:


- [by using the Deployment Wizard to create a new HTML file.](#)
- [by adding the `TraceOptions` parameter to the `APPLET` tag in an HTML file.](#)

Using the Deployment Wizard to add the `TraceOptions` parameter to a new HTML file

1. Create a new HTML session file that includes the problem determination components.
 1. Click Advanced Options on the Additional Options panel.
 2. Click the Other tab. Click Yes to include the problem determination components.
 3. Click OK.
 4. Finish to create the new session HTML file.
2. Edit the session HTML file you created to add the `TraceOptions` parameter.
 1. Start the [Deployment Wizard](#) and open the new HTML file you have created.
 2. Click Next to reach the Additional Options panel, click Advanced Options, then select the Other tab.
 3. Type `TraceOptions` in the Name field.
 4. Type `"SaveLocation=Local,OutputFile=c:\temp\trace.tlg,HOD.Session=3"`, excluding the quotes, in the value field. `OutputFile` can be any valid file name.
 5. Click set. The parameter is added to the Additional Parameters list.
 6. Click OK to return to the Additional Options page, and finish editing the HTML file.

Adding the `TraceOptions` parameter to the `APPLET` tag of a session HTML file

The `TraceOptions` parameter has already been added to the `APPLET` tag of the Cached client with problem determination (`HODCachedDebug.html`) and the Download client with problem determination (`HODDebug.html`), but is commented out. Use a text editor to uncomment the `IPMonitor` parameter to use the parameter with either of these clients.

 You can only use the Deployment Wizard to edit files that you have created with the Deployment Wizard. You cannot use the Deployment Wizard to edit the Cached client with problem determination or the Download client with problem determination.

To add the `TraceOptions` parameter to HTML files you have created without using the Deployment Wizard, use a text editor to edit the HTML file. The session must first include the problem determination components. Change:

```
<APPLET archive="hod.jar,sccbase.jar" CODE="com.ibm.eNetwork.HOD.HostOnDemand.class"
WIDTH=584 HEIGHT=450>
```

to:

```
<APPLET archive="hoddbg.jar,sccbase.jar"
CODE="com.ibm.eNetwork.HOD.HostOnDemand.class" WIDTH=584 HEIGHT=450>
```


and add add the following parameter to the applet tag:

```
<PARAM NAME=TraceOptions VALUE="[<option_tag=<option_value>,...]">
```

For example,

```
<PARAM NAME=TraceOptions
VALUE="SaveLocation=Local,OutputFile=c:\temp\trace.tlg,HOD.Session=3">
```

would start the trace facility, trace the `HOD.session` module at level 3, and save the trace file to `c:\temp\trace.tlg` on the client.

 Enclose the string that follows `VALUE=` in quotes. Without quotes, the Host On-Demand server stops parsing the string as soon as it reaches a space. This may cause some of the `TraceOptions` settings you want to set to be discarded by the Host On-Demand server.

There is also a sample file, `cmprtrace.html` that can show you how to use this parameter. It is located in the `x:\hostondemand\hod\ibmserv` directory.

Trace Option	Supported Values	Description
Functions, Components, and Levels	HOD.JNIload=1,2,3 HOD.PrtTerminal=1,2,3 HOD.Macro=1,2,3 HOD.Session=1,2,3 HOD.BlinkRemapModel_Trace=1,2,3 HOD.ImportExport=1,2,3 HOD.ColorRemapModel3270_Trace=1,2,3 HOD.Screen=1,2,3 HOD.Config=1,2,3 HOD.FUDOMA=1,2,3 HOD.Keypad=1,2,3 HOD.ColorRemap=1,2,3 HOD.CodePage=1,2,3 HOD.MacroManager=1,2,3 HOD.KeyRemap=1,2,3 HOD.FileTransfer=1,2,3 HOD.ServiceLocationProtocol=1,2,3 HACL.Printer=1,2,3 HACL.ECLScreenReco=1,2,3 HACL.ECLField=1,2,3 HACL.ECLErr=1,2,3 HACL.ECLOIAEvent=1,2,3 HACL.Transport=1,2,3 HACL.ECLOIA=1,2,3 HACL.ECLSession=1,2,3 HACL.ECLPS=1,2,3 HACL.DataStream=1,2,3 HACL.ECLScreenRecoEvent=1,2,3 HACL.ECLCommEvent=1,2,3 HACL.ECLPSEvent=1,2,3 HACL.ECLScreenDesc=1,2,3 HACL.ECLXFer=1,2,3 HACL.ECLRecoDebugEvent=1,2,3 HACL.ECLFieldList=1,2,3	Host On-Demand components that can be traced. Contact IBM Service for which modules to trace. The numbers 1, 2 and 3 indicate the type of message logged: 1 for Informational, 2 for Warning and 3 for Error.
Save Location	SaveLocation=Server,Local	Determines if the trace file is saved on the client machine or on the Host On-Demand server machine. If SaveLocation is not specified, the trace file is saved on the Host On-Demand server machine in the <code>private</code> directory as <code>SVRLOGANDTRACE.[user_name].user</code> , where <code>user_name</code> is the user ID used to logon to the Host On-Demand session.
Local output file	OutputFile=x:\filename.trc	Specifies the trace file name and location when SaveLocation=Local. When SaveLocation=Server, the file is saved to the Host On-Demand server in the <code>private</code> directory as <code>SVRLOGANDTRACE.[user_name].user</code> , where <code>user_name</code> is the user ID used to logon to the Host On-Demand session.
Number of trace entries	NumberOfTraceEntries=1024	Limits the number of trace entries in the trace file.

Related topics:

- [The TraceOptions HTML parameter](#)
- [The IPMonitor HTML parameter](#)
- [IP Monitor](#)
- [Viewing a User's Trace](#)
- [Tracing on the Server](#)
- [Tracing on the Client](#)
- [Log and Trace Messages Format](#)
- [Setting Trace Levels](#)
- [Changing the trace settings \(client\)](#)

IPMonitor is a Java utility you can use to collect trace information containing the session data flowing between a client and a host. IPMonitor is an intermediary between a client and a host. The client connects to IPMonitor, while IPMonitor connects to the host. IPMonitor then records session data flowing between the client and the host. You can use IPMonitor as a Java application or as a Java applet.

- IPMonitor v1.0 for Java is a Java application that runs on the Host On-Demand server. To collect and save a trace using this version of IPMonitor, the system administrator must:
 - assist the user in configuring the client to connect to IPMonitor, by modifying the session properties
 - configure IPMonitor to connect to the host
 - start IPMonitor on the server
 - start the client after IPMonitor is started on the server

before you can recreate the problem and capture the trace information. The user does not need to send the trace file to the admin because the trace is stored on the Host On-Demand Server.



IPMonitor captures encrypted data and plays it back properly, but since the data is encrypted, it cannot be used for debugging. In order to debug the trace properly, before you run the IPMonitor, you must disable SSL in the session that is used for the trace. If SSL is not turned off, the data captured by IPMonitor will be encrypted and will not be usable for problem determination. To turn off SSL, do the following:

1. End the session.
 2. Open the session Properties.
 3. Go to the Security tab, and set Enable Security (SSL) to No.
 4. Save the session Properties.
- IPMonitor v1.0 for Java, automatic mode and IPMonitor v1.0 for Java, normal mode are Java applets that run on the client. The applet establishes the connection between the current client and itself, so you do not have to modify session properties as you must do to start IPMonitor as an application. Using the IPMonitor applet, the system admin and the user do not need to work at the same time to collect the trace.

Differences between automatic mode and normal mode include:

- You start IPMonitor in automatic mode by right clicking on the session's icon on the desktop, and selecting Start Session with IPMonitor. The HTML file you use to start the session must include the `IPMonitor` HTML parameter, and must include the problem determination components. As a Host On-Demand Administrator, you can modify an HTML file so that a user can access it. The user can recreate the problem and capture trace information without your involvement. IPMonitor in automatic mode starts automatically immediately after the session starts.

While this version of IPMonitor is easier for the user to use and involves less administrative effort, the user is locked into the host, port and trace file path specified in the HTML file.

- You start IPMonitor in normal mode by selecting Actions > Run Applet from the Host On-Demand session menu. The user must know and type the class name for the applet when the Run Applet window appears. IPMonitor in normal mode must be started manually after the session is connected.

While this version of IPMonitor allows greater flexibility in changing the host or port to trace, there is more administrative effort to configuring IPMonitor.

Related topics:

- [IPMonitor v1.0 for Java](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)

- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)



Tracing on the server

Starting and stopping a trace

For a user

To capture a user trace to be viewed in the Host On-Demand administrator window, log on to the Host On-Demand client as the user. Follow the [steps](#) for starting and stopping a trace on the Host On-Demand client. Make sure you set the save location to Server.

1. Click Settings.
2. Select Server for the save location.
3. Click OK.

For a service

To capture a service trace:

1. Click Services.
2. Select the service and click Start Trace. Make sure the service is started.
3. Take the necessary steps to reproduce the problem. Trace messages for the service are logged.
4. Stop the trace by clicking Stop Trace.

Viewing a log or trace file

Tracing and logging are always on for the server. Both log and trace messages are captured and displayed in the console. If tracing is turned on for a service, trace and log messages for that service are also displayed. If tracing is turned off for all services, only server messages are displayed.

To view the server trace file, click the Service and then click Server Log.

To view a service trace file after tracing has been started, click the Service and then click Server Log.

To view a user's trace file on the server after a trace is captured and saved to the server:

1. Select a user.
2. Right-click and select Trace Facility.

To refresh the messages in the console, click File > Refresh.

Related topics

- [Setting trace levels](#)
- [Log and trace messages](#)

Log and trace messages format



[message type][message number][time stamp][function name][component][correlator]message text

message type

indicates the type of message logged: 1=Information, 2=Warning, 3=Error, and 4=Trace

message number

increasing message record number

time stamp

date/time the event was logged

function name

function that logged the event

component

component that logged the event

correlator

a key that groups log records

message text

text of the log or trace message

Related topics

- [Using the trace facility](#)
- [Setting trace levels](#)
- [Viewing a log file](#)

IPMonitor v1.0 for Java



IPMonitor v1.0 for Java is a Java application that you can use to collect trace information containing the data flowing between a client and a host. The IPMonitor window displays:

Client

Identifies the Host On-Demand server that the client connects to. IPMonitor runs on the same server. The name is specified in the Destination Address field of the session properties.

Port

Identifies the port on the Host On-Demand server that the client uses to connect to IPMonitor. The port is specified in the Destination Port field of the session properties. You can edit this field.

Connection status

Displays the status of the connection between the client and IPMonitor. Status is dynamically updated when you connect or disconnect the client from IPMonitor.

Host

Specifies the name of the host that IPMonitor connects to. You can edit this field.

Port

Identifies the port that IPMonitor uses to connect to the host. You can edit this field.

Connection Status

Displays the status of the connection between the host and IPMonitor. Status is dynamically updated when you connect or disconnect IPMonitor from the host.

Trace file

Displays what the name and directory location of the trace file will be when the trace is saved. You can edit this field.

Start/Stop

Starts or stops the IPMonitor trace.

Connect/Disconnect

Connects or disconnects the session.

Save

Saves the trace information to the listed trace file.

Related topics:

- [IPMonitor](#)
- [Configuring the IPMonitor v1.0 for Java application](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)

Starting the IPMonitor v1.0 for Java application

For Windows NT and Windows 2000 Host On-Demand servers, the command file to run the IPMonitor utility is installed in the `hostondemand\lib\samples\IPMonitor` directory when Host On-Demand is installed. The command file is called `IPMon.cmd`, and it is the only file installed on Windows Host On-Demand servers.

For other operating systems running Host On-Demand servers, all the script files to run the IPMonitor utility are installed in the `hostondemand\lib\samples\IPMonitor` directory. Script files include:

- `IPMon-AIX` for AIX
- `IPMon-Novell.cnf` for Novell
- `IPMon-OS2.cmd` for OS/2
- `IPMon-UNIX` for HP-UX, Linux, and Solaris

To start the IPMonitor utility, type the following at the command line (be sure to use the parameters in the correct order):



```
IPMon-xxx [hostname] [host port] [local port]
```

where:

- `IPMon-xxx` is the IPMonitor utility command or script file for your operating system.
- `hostname` is the name of the remote host. If this parameter is omitted, the default hostname is *unknown*.
- `host port` is the port for the remote host. If this parameter is omitted, the default port is 23.
- `local port` is the port for the IPMonitor utility. If this parameter is omitted, the default is 8888.

For example, on AIX you could run:

```
IPMon-AIX vmhost 23 8888
```

where `vmhost` is the hostname of the host connection you want to trace, 23 is the host port, and 8888 is the local port for IPMonitor.

If you do not specify any parameters when you start the IPMonitor utility, you can type in values for the parameters when the IPMonitor window appears.

Related topics:

- [IPMonitor](#)
- [IPMonitor v1.0 for Java](#)
- [Configuring the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)

IPMonitor v1.0 for Java, automatic mode

The IPMonitor v1.0 for Java, automatic mode, is an applet that runs on the Host On-Demand client, and collects trace information containing the session data flowing between a client and a host.



IPMonitor in automatic mode connects the to the client and to the host. You can click Action > Disconnect/Connect on the session menu to disconnect or re-connect the client with IPMonitor.

The IPMonitor window displays:

Host

Contains the host name of the host that the client connects to. IPMonitor in automatic mode obtains this information automatically from the session properties. You cannot edit this field.

Port

Identifies the port the client uses to connect to the host. IPMonitor in automatic mode obtains this information automatically from the session properties. You cannot edit this field.

Connection Status

Displays the status of the connection between the IPMonitor and the host. Connection status is dynamically updated when you connect or disconnect the session.

Trace file

Displays the name and directory location of the trace file, which is specified by the `IPMonitor` parameter in the HTML file. You cannot edit this field.

Trace status

Displays the status of the IPMonitor trace. Trace status is dynamically updated when you click Start/Stop.

Start/Stop

Starts or stops the IPMonitor trace.

Clear

Erases all trace information from memory. IPMonitor accumulates trace information in memory, and does not write any information to the trace file until you click Save and Exit.

Save and Exit

Saves the trace information to the listed trace file, closes the IPMonitor window, disconnects the session from the host, but does not close the host session window. Click Communication > Connect on the session menu to reconnect to the host without starting the IPMonitor.

Related topics:

- [IPMonitor](#)
- [IPMonitor v1.0 for Java](#)
- [Configuring the IPMonitor v1.0 for Java application](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)

Configuring IPMonitor v1.0, automatic mode



IPMonitor v1.0 for Java, automatic mode is a Java applet that you can use to collect trace information containing the session data flowing between a client and a host. You can access it from the Start Session with IPMonitor option on the session icon's start menu. This option is available after you have added the `IPMonitor` parameter to the session HTML file. Host On-Demand servers running on Win32, AIX, Sun Solaris, OS/2, Novell Netware, OS/400, MVS/390 and Linux all support the `IPMonitor` parameter, however, only 3270 display, 5250 display and VT display sessions support IPMonitor tracing.

You can add the `IPMonitor` parameter to session HTML files in two ways:


- [by using the Deployment Wizard to create a new HTML file.](#)
- [by adding the `IPMonitor` parameter to the APPLET tag in an HTML file.](#)

Using the Deployment Wizard to add the IPMonitor parameter to a new HTML file

1. Create a new HTML session file that includes the problem determination components.
 1. Click Advanced Options on the Additional Options panel.
 2. Click the Other tab. Click Yes to include the problem determination components.
 3. Click OK.
 4. Finish creating the new session HTML file.
2. Edit the session HTML file you created to add the `IPMonitor` parameter.
 1. Start the [Deployment Wizard](#) and open the new HTML file you have created.
 2. Click Next to reach the Additional Options panel, click Advanced Options, then select the Other tab.
 3. Type `IPMonitor` in the Name field.
 4. Type `"SessionName=My Session,TraceFile=c:\mydirectory\trace.trc"`, excluding the quotes, in the value field. `SessionName` can be any session name available on the Host On-Demand desktop. The `SessionName` must be spelled *spelled exactly as it appears* in the session properties, and as it is displayed below the session icon, including spaces. `TraceFile` can be any valid file name.
 5. Click set. The parameter is added to the Additional Parameters list.
 6. Click OK to return to the Additional Options page, and finish editing the HTML file.

Adding the IPMonitor parameter to the APPLET tag of a session HTML file

The `IPMonitor` parameter has already been added to the APPLET tag of the Cached client with problem determination (`HODCachedDebug.html`) and the Download client with problem determination (`HODDebug.html`), but is commented out. Use a text editor to uncomment the `IPMonitor` parameter to use the parameter with either of these clients.

 You can only use the Deployment Wizard to edit files that you have created with the Deployment Wizard. You cannot use the Deployment Wizard to edit the Cached client with problem determination or the Download client with problem determination.

To add the `IPMonitor` parameter to HTML files you have created without using the Deployment Wizard, use a text editor to edit the HTML file. The session must include the problem determination components. Change:

```
<APPLET archive="hod.jar,sccbase.jar" CODE="com.ibm.eNetwork.HOD.HostOnDemand.class"
WIDTH=584 HEIGHT=450>
```

to:

```
<APPLET archive="hoddbg.jar,sccbase.jar"
CODE="com.ibm.eNetwork.HOD.HostOnDemand.class" WIDTH=584 HEIGHT=450>
```


and add the following parameter to the applet tag:

```
<PARAM NAME=IPMonitor VALUE="[<option_tag=<option_value>,...]">
```

For example,

```
<PARAM NAME=IPMonitor VALUE="SessionName=My
Session,TraceFile=c:\mydirectory\trace.trc">
```

adds the option Start Session with IPMonitor to the menu when you right click the icon for the session named "3270 to myhost" on the Host On-Demand desktop. Selecting this option starts the session and also starts IPMonitor. The trace file is saved to c:\mydirectory\trace.trc.

 Enclose the string that follows VALUE= in quotes. Without quotes, the HTML parser stops parsing the string as soon as it reaches a space. This may cause some of the IPMonitor settings you want to set to be discarded by the HTML parser.

There is also a sample file, ipmon.html that can show you how to use this parameter. It is located in the x:\hostondemand\lib\samples\IPMonitor directory.

Trace Option Supported Values

SessionName Any session name available on the Host On-Demand desktop, *spelled exactly as it appears* in the session properties, and as it is displayed below the session icon.

TraceFile Any valid file name.

Description

Specifies the name of the session that you want to have started along with IPMonitor. If no session name is specified, IPMonitor can be run by all 3270 display, 5250 display, and VT display sessions defined for the Host On-Demand desktop you logged on to.

Specifies the trace file name that the IPMonitor trace is saved to. If no file name is specified, IPMonitor saves the trace file to output.tlg in the path specified in the JVM system property "user.dir".

When you select Start Session with IPMonitor from the session icon's start menu, the [IPMonitor v1.0 for Java, automatic mode](#) appears first, and then the session starts.

Related topics:

- [IPMonitor](#)
- [IPMonitor v1.0 for Java](#)
- [Configuring the IPMonitor v1.0 for Java application](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)

IPMonitor v1.0 for Java, normal mode



The IPMonitor v1.0 for Java, normal mode, is an applet that runs on the Host On-Demand client, and collects trace information containing the session data flowing between a client and a host.

The IPMonitor window displays:

Host

Identifies the host name, specified in the session properties, of the session that IPMonitor is tracing. You can edit this field. To switch to another host of the same session type, click Disconnect, type the new host name into the Host field, then click Connect.

Port

Identifies the port, specified in the session properties, that the session is using to communicate to the host. You can edit this field. To switch to another port on the same host, click Disconnect, type the new port number into the Port field, then click Connect.

Connection Status

Displays the status of the connection between the IPMonitor and the host. Connection status is dynamically updated when you connect or disconnect the session.

Trace file

Displays the name and directory location of the trace file, which is specified by the `IPMonitor` parameter in the HTML file. You can edit this field.

Start/Stop

Starts or stops the IPMonitor trace.

Connect/Disconnect

Starts or stops the session between IPMonitor and the host, and the session between the IPMonitor and the client.

Save

Saves the trace information to the listed trace file.

Related topics:

- [IPMonitor](#)
- [IPMonitor v1.0 for Java](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)

Starting IPMonitor v1.0 for Java, normal mode

You can [start IPMonitor v1.0 for Java, normal mode](#), from the Run Applet session menu option. It doesn't need to be configured before starting, like IPMonitor v1.0 for Java, automatic mode or the IPMonitor v1.0 for Java application. IPMonitor v1.0 for Java, normal mode receives host name, host port and trace file location from the active session. You can modify host name, host port and trace file location to [trace another session](#).

Starting IPMonitor v1.0 for Java, normal mode

1. Start a 3270 display, 5250 display or VT display session. Wait for the session to connect.
2. Select Actions > Run Applet from the session menu bar.
3. Type the following *exactly* as it appears below in the Run Applet window in the Enter class name field:

```
com.ibm.eNetwork.HOD.util.IPMonitor.IPMonitor
```

4. Click Run to launch the IPMonitor applet. The IPMonitor window appears.
5. Recreate the problem in the session that you want to gather trace information about.
6. Click Stop to end the trace once you have reproduced the problem, then click Save to save the trace data to the file listed in the Trace File: field.
7. Close IPMonitor v1.0, normal mode and close the session.

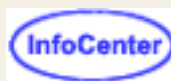
Modifying IPMonitor v1.0 for Java, normal mode to trace a different session

1. After starting [IPMonitor v1.0 for Java, normal mode](#), click Disconnect end IPMonitor's connection with the host.
2. Modify the host name, port or trace file location, then click Connect. IPMonitor makes the connection using the modified information.
3. Recreate the problem in the session that you want to gather trace information about.
4. Click Stop to end the trace once you have reproduced the problem, then click Save to save the trace data to the file listed in the Trace File: field.
5. Close IPMonitor v1.0, normal mode and close the session.

Related topics:

- [IPMonitor](#)
- [IPMonitor v1.0 for Java](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)

Configuring the IPMonitor v1.0 for Java application



IPMonitor v1.0 for Java is a Java application that you can use to collect trace information containing the session data flowing between a client and a host. IPMonitor runs on the Host On-Demand server and connects to the host, so that the client can establish a host session through IPMonitor.

If users are allowed to modify session properties, they can follow the steps below. If users are not allowed to modify session properties, the system administrator will need to follow the steps below for the user

1. [Start the IPMonitor application](#) on the server. If you did not start IPMonitor with the host name, host port, and local port parameters, enter this information into the IPMonitor window.
2. Right click on the session icon on the client desktop, accessed through the client's browser, and select Properties.
3. Set the Destination Address to the TCP/IP address of the Host On-Demand server that will run the IPMonitor application. For example, if the Host On-Demand server's name is `hodserv1`, and its TCP/IP address is 10.27.70.115, you can specify either `hodserv1` or 10.27.70.115 in this field.
4. Set the Destination Port the same as the value specified for the local port in the IPMonitor application configuration. The default port is 23.
5. Click Connect in the IPMonitor window on the server where IPMonitor was started. The Connect button changes to Disconnect and the Connection status to the client changes to Waiting.
6. Start the Host On-Demand session on the client that you have configured to connect to the IPMonitor application. The session window appears with data from the host, just as if you were connected directly to the host. In the IPMonitor window on the server, the client and host Connection status both change to Connected.
7. Recreate the problem on the client workstation for which you want to gather trace information.
8. Click Stop on the server, in the IPMonitor window, to end the trace once you have reproduced the problem, then click Save to save the trace data to the file listed in the Trace File: field.
9. Close IPMonitor on the server and close the session on the client workstation.

Related topics:

- [IPMonitor](#)
- [IPMonitor v1.0 for Java](#)
- [Starting the IPMonitor v1.0 for Java application](#)
- [IPMonitor v1.0 for Java, automatic mode](#)
- [Configuring IPMonitor v1.0 for Java, automatic mode](#)
- [IPMonitor v1.0 for Java, normal mode](#)
- [Starting IPMonitor v1.0 for Java, normal mode](#)

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:

- The [name](#) of the printer session
- The Session ID or shortname
- The printer [LU name](#) (3270)
- The LU Name of the [associated display session](#), if any (3270)
- Workstation ID (5250)

For example, if the title of the window appears as:

Myprinter - B - MyprinterLU - MydisplayLU33 (3270)

Myprinter - B - WorkstationID (5250)

The printer status window displays the status of the:

- [Session](#)
- [Print job](#)
- [Printer or file](#)

The [OIA](#) (Operator Information Area) also displays if you specify it in the configuration.

From the menu bar, you can:

- Jump to the next session or close the session.
- Turn the graphic display on or off.
- Stop or Start the session.
- View the message log or run a trace.
- Print a test page or eject a page (3270).
- Open the Page Properties window (3270).

The pushbuttons at the bottom of the window vary according to the way the session was configured. On a 3270 session, there can be a PA1 and a PA2 button, depending on the configuration, but there are always Cancel Job and Help buttons.

- PA1 and PA2 (Program Attention) keys - provide a means of communicating with the host application program if the program has defined them. (3270)
- Cancel Job - cancels the job that is currently being sent from the host.
- Help - provides help for this window.

Checking and upgrading the JVM level for Microsoft Internet Explorer

You must have JVM level 3165 or later installed in order to use Microsoft Internet Explorer with Host On-Demand V6 or later. To determine what JVM level is currently installed, you can view Internet Explorer's Java console by selecting View > Java console, if you have enabled the Java console display.

To enable the Java console display:

- Select Tools > Internet options.
- On the Advanced tab, under Microsoft VM, select Java console enabled.
- Click Ok to save your changes.
- Shut down and restart Windows.

If you need to update the JVM, you can either:

- Download an updated JVM for your installed version of Internet Explorer from Microsoft.
- Install one of the supported levels of Internet Explorer (4.01 with SP1, 5.0 and 5.01), choose Custom Installation during installation and select Update JVM. **Note:** Selecting a Typical Installation of Internet Explorer does not update the level of a pre-installed JVM.

Connection tab



[Session Name](#)

[Destination Address](#)

[Destination Port](#)

[Enable SLP](#)

[TN3270E](#) (3270 display session)

[LU or Pool Name](#) (3270)

[Screen Size](#)

[Host Code-Page](#)

[Associated Printer Session](#) (3270 display session)

[Close Printer With Session](#)

[Workstation ID](#) (5250 session)

[AS/400 Name \(SLP\)](#) (5250 session)

[CICS Server \(CICS gateway session\)](#)

[CICS-Gateway Code-Page \(CICS gateway session\)](#)

[Print-Buffer Size](#) (3270 printer session)

[File Transfer Type \(3270 and 5250 display session\)](#)

[Lock](#)

Session Name

The name you want your session to have. The name appears beneath the session's icon and at the top of the session window.

Destination Address

The host name or TCP/IP address of the telnet server to which you want the session to connect. This can be the Host On-Demand server (if the session will connect through the Redirector), a communications server/gateway or a host system.

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

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.

The default port is 23 for 3270, 5250 and VT, and 2006 for CICS.

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 port used by the display session.

Enable SLP

Enables you to dynamically find a service without knowing the destination port and address. Your network must be configured to support [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 logical unit (LU) name when establishing a connection, so you can use only pool names.

AS/400 Name (SLP)

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 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 #.

Workstation ID

Defines the name of this workstation. 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, \$, @, #, . (period), and _ (underscore). If you do not complete this field, a workstation ID is automatically defined by the host.

The Telnet 5250 client can generate a new and non-arbitrary Workstation ID for a session without requiring per-session customization or a user exit. Keywords and special characters in the Workstation ID field can cause some or all of the following information to be substituted into the Workstation ID value that is sent to the TN5250 server:

- Computer name or User name (&COMP, &USER)
- short Session ID(*)
- Session Type ID(%)
- Collision Avoidance ID(=)

When specified, the Collision Avoidance ID enables the generation of a new Workstation ID if the Telnet server rejects the previous name (which can occur when the old name is already in use on the AS/400).

TN3270E

If the server/gateway or host system to which the session will connect does not support the TN3270E (Enhanced) protocol, click No. The Enhanced protocol lets you specify the LU or LU Pool to which the session must connect and, if necessary, an associated printer session. In addition, the Enhanced protocol supports the Network Virtual Terminal (NVT) protocol, which lets you connect to servers in ASCII mode. For example, you can use this to log on to a firewall.

LU or Pool Name

You can specify the name of an LU or LU Pool, defined at the telnet server, to which the session must connect. If you do not specify an LU or pool name, the result depends on the type of server to which the session is connecting. If you are connecting to Communications Server/390 V2R10, you can enter the name of a LUGROUP for the POOL name.

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.

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 #.

Screen Size

Defines the number of rows and columns in the session screen. Click the arrow next to the field to see the choices.

The default is 24x80.

Print-Buffer Size

The size of the block of memory reserved for print data that is being sent to the printer. The valid values are in the drop-down list. This applies only to LU3 sessions.

The default Print-Buffer Size is 1920.

Host Code-Page

Specifies the table used to map EBCDIC codes from the host to appropriate ANSI graphics on the workstation. Click the arrow next to the field to see the choices, which vary according to the session type. The default is the code page that corresponds to the locale for which your workstation is configured. You must set it to the code page supported by the host system to which the session will connect.

Associated Printer Session

You can associate a 3270 printer session with a 3270 display session. *Make sure the association has been correctly configured at the Telnet server.*

Choose a printer from the pull-down list, which includes printer sessions that are configured for this user.

If an SLP-enabled display session is configured with an associated printer, regardless of whether or not the printer session is configured for SLP, an associated printer session is started with the telnet server found for the display session.

If a printer session contains a destination address but no LU name and the session is started independently of the display session, Host On-Demand attempts to create an associated printer session with an active display session going to the same destination address.

Close Printer With 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 this option is set to Yes, 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.

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.

CICS Server

The name of the CICS server to which the session connects. If this field is blank, the CICS Gateway's default server is used.

CICS Gateway Code-Page

The code page in use by the operating system at the CICS Gateway. If this field is set to 000 Auto-detect, Host On-Demand normally retrieves the code-page setting from the CICS Gateway; if that is not possible, you must get the correct code page from the network administrator.

File Transfer Type

Determines if the file transfer type is Host File Transfer or FTP. If File Transfer Type is FTP a separate FTP session is started from the display session.

Note: Screen Customizer does not support the FTP client, so if the Screen Customizer session property is enabled in a display session's properties then the supported File Transfer Type is Host File Transfer, not FTP.

Also note that FTP sessions do not support SSL even if the session is configured for SSL.

The default is Host File Transfer.

Lock

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

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.
- **PROG nnn** - Indicates an error in the print datastream from the host system. Note the specific number (nnn), then use the "?" button to get 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.

Print job status



- 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)
- Printing - Indicates that the print job is currently being printed. (5250)
- Canceling - Indicates that the user has pushed the Cancel Job button. 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. **Note:** This can take awhile 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.

Service Location Protocol (SLP)



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. Host On-Demand 3270 and 5250 sessions can use SLP to automatically discover TN3270 and TN5250 telnet servers in a network. The Host On-Demand client then uses load information returned from the server to connect through the server carrying the least session load at the time the connection is attempted.

For additional important information on SLP and session balancing, refer to [RFC 2165 Service Location Protocol](http://www.ietf.org/rfc/rfc2165.txt) at <http://www.ietf.org/rfc/rfc2165.txt>, and [draft RFC TN3270E Service Location and Session Balancing](http://www.ietf.org/internet-drafts/draft-ietf-tn3270e-service-loc-06.txt) at <http://www.ietf.org/internet-drafts/draft-ietf-tn3270e-service-loc-06.txt>.

 If Enable Security (SSL) on the Security tab is set to Yes, a connection can be established only to servers that support Secure Sockets Layer Version 3 security.

[SLP Administration](#)

[Directory agent support](#)

[SLP limitations](#)

[Server support and limitations](#)

[Tuning the network](#)

[SLP requirements to run on a token ring](#)

SLP Administration

A client or User Agent (UA) attempts to discover the location of a service by multicasting a service request to the service location general multicast address 224.0.1.22. Service Agents (SAs) that satisfy the UA request and that are listening to this address send a service response. Directory Agents (DAs) will respond on behalf of the SAs when a network contains directory agents.

See [RFC 2165 Service Location Protocol](#) for an explanation of UA, DA, and SA terminology, and for a description of the SLP network.

Directory agent support

Host On-Demand supports a network that includes DA, as well as SAs, processing of the service requests. SAs register the services and attributes of these services with a DA.

Clients can learn where the DAs are and unicast service requests to a DA, instead of multicasting to the service-specific multicast address.

DA support is relevant in a large installation that needs to reduce network traffic.

Attributes

Host On-Demand is the user agent and sends the SLP service request according to the session type you are starting. For example, if you have enabled SLP and are connecting a 3270 Display or Printer session, the requested service will be tn3270.

The Host On-Demand service types that can be requested are tn3270 or tn5250. The service requests can be delimited by these attributes:

[SCOPE](#)

[LOAD](#)

[SECURITY](#)

LUPOOL

AS400NAME

SCOPE

SCOPE is a collection of services that make up a logical group. Host On-Demand includes SCOPE in a service request when a value is specified in the Scope field on the Advanced tab during session configuration. If Scope is not included, only unscoped servers respond.

LOAD

LOAD is a value returned by the server on an attribute request. It is an integer number between 0 and 100. Load calculations vary among different server types and may return inconsistent values. Host On-Demand balances the sessions by connecting to the server that returns the lowest value for the load attribute. Servers can be adjusted to compensate for differences in load balancing calculations. Administrators should refer to the server documentation for additional information.

SECURITY

Host On-Demand includes SECURITY in the service request if Enable Security (SSL) is set to Yes on the Security tab during session configuration. When SSL is enabled, the value of the SECURITY attribute is SSLV3. When SSL is not enabled, the value of the SECURITY attribute is NONE. Only servers that support the requested level of security will respond to the level of service request.

LUPOOL

LUPOOL is included in the service request if LU Name or Pool is specified on the Connection tab during session configuration. Only pool names are valid for SLP.

AS400NAME

AS400NAME is included in the service request if SLP AS/400 Name is specified on the Connection tab during session configuration. If an SLP AS/400 name is specified, the connection is established to that AS/400; otherwise, the connection is made to the AS/400 configured as the default at the server.

SLP limitations

- When SLP is enabled, you can use only pool names. LU names cannot be used.
- The environment used for SLP must support multicast. Broadcast is not supported.
- Directory Agent Discovery timeout and Service Agent Multicast timeout are not separately configurable.

Browser limitations:

- SLP is not supported on Linux with Netscape.
- A session may fail to connect because Telnet Service or Directory Agents cannot be found. A limitation of the Netscape browser may restrict the Time to Live (TTL) range of the SLP packets to 1 instead of the standard setting of 32 for site-wide coverage. This limits the number of routers that the SLP discovery packets can be passed through before the packets are dropped. This is caused by a limitation of the JVM that is shipped with the Netscape browser. Use another browser that supports TTL settings of 32.

Server support and limitations

Supported servers

- IntraNetWare for SAA 3.0 (or later)
- Communications Server for Windows NT 6.0 (or later)

It is recommended that all SLP servers in the network be defined as scoped. The following fixes must be applied to get responses from both scoped and unscoped servers when no value or the default is entered for the scope: NetWare for SAA 3.0 JR12403 and CSNT 6.0 JR13234.

Server limitations

- Communications Server for Windows NT 6.0 does not support Telnet 5250 Enhanced; therefore, you can connect only 5250 display sessions, and they do not support the Workstation ID. 5250 printer sessions cannot be connected.
- IntraNetWare for SAA 3.0 does not support Telnet 5250 display or printer sessions or SSL.
- IntraNetWare for SAA 4.0 does not support Telnet 5250 Enhanced; therefore, you can connect only 5250 display sessions, and they do not support the Workstation ID. 5250 printer sessions cannot be connected through this server.

Tuning the network

Refer to load and session balancing in the Server documentation for more specific information on tuning the network.

Refer to [draft RFC TN3270E Service Location and Session Balancing](#) for additional information on load.

Refer to [RFC 2165 Service Location Protocol](#) for information on scalability issues regarding how scope is used and how a DA can be used in a network.

SLP requirements to run on a token ring

SLP uses IP multicast to find the location of the telnet servers. On a token ring, three methods exist for mapping between an IP multicast address and a hardware address (rfc 1469):

- The all rings broadcast address
- The assigned functional address
- The existing IEEE assigned IP Multicast group addresses

For SLP to work properly on a token ring, all hosts on the ring must agree on the same method for mapping. Currently, only the first and second methods are implemented.

If the second method is available, a configuration option probably has been added for the first method for backward compatibility. To switch between the methods, follow the steps for your platform.

[AIX](#)

[OS/2](#)

[Windows 2000](#)

AIX

To check what method is being used:

```
no -a | grep multi
```

A value of 1 for `ie5_old_multicast_mapping` is for all rings broadcast address and a value of 0 is for assigned functional address. The default is 0. To change the value:

```
no -o ie5_old_multicast_mapping=1
```

Do not use additional spaces between the keyword, the equals sign, and the value. To make the value permanent, add the command to the `rc.net` file located in the `etc` directory.

OS/2

To change the value on OS/2, use `ifconfig`. To determine the correct command for the OS/2 version you are using:

```
ifconfig -?
```

To change the value to the all rings broadcast address:

```
ifconfig [interface] multibc
```

or

```
ifconfig [interface] m_cast BC
```

To change the value to the assigned functional address:

```
ifconfig [interface] multifa
```

or

```
ifconfig [interface] m_cast FA
```

To make the value permanent, add the ifconfig statement to setup.cmd located in the **\mpn\etc** directory.

Windows 2000

To change the value on Windows 2000, edit the TCP/IP parameter in the Registry as follows:

Parameter:

TrFunctionalMcastAddress

Key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Value Type:

REG_DWORD-Boolean

Valid Range:

0, 1 (False, True) (0=All rings broadcast address, 1=Assigned functional address)

Default:

1 (True)

Description:

This parameter determines whether IP multicasts are sent using the Token Ring Multicast address as described in RFC 1469 or using the subnet broadcast address. The default value of 1 configures the computer to use the RFC1469 Token Ring Multicast address for IP multicasts. Setting the value to 0 configures the computer to use the subnet broadcast address for IP multicasts.

Adding sessions

There are two ways to create a new session:

1. Create a new session by duplicating a default session.
2. [Import a session](#) from your computer's file system.

To copy a default profile:

1. Right-click the icon for the profile you want to copy.
2. Click Copy.
3. Click Close.
4. To configure the session, right-click the new icon in the Configured Sessions area, then click Properties.
5. Configure the parameters, then click OK.

The default sessions in this window were created for you, or for the groups of which you are a member, by your system administrator. You can create a new session by copying any of the default sessions to the Configured Sessions area in the Client window and then modifying it as necessary. The new session is saved in your account and is available whenever you log on (unless the administrator has chosen not to let you save preferences).

You cannot delete the sessions in this window.

Related topics

- [Importing sessions](#)
- [Exporting sessions](#)

Starting sessions with bookmarks or icons

[Creating a bookmark to bypass the logon window](#)

[Creating a bookmark that automatically starts a host session](#)

[Creating a desktop icon for a bookmarked session](#)

A security warning window may appear while you are using Host On-Demand. The content of the window depends on your browser. The purpose of the window is to tell you that Host On-Demand was created by **International Business Machines** and to ask whether you trust it. You must click Grant or Yes to continue. To stop the window from reappearing, click:

- Remember this decision (Netscape).
- Always trust content from International Business Machines (Microsoft Internet Explorer).

Creating a bookmark to bypass the logon window

1. Click Start > Programs > IBM Host On-Demand > Administration.
2. Click Clients and Utilities.
3. Click the Host On-Demand client you want to start.
4. Enter your user ID and password, then click Log On.
5. After successfully logging on, create a bookmark for the page using your browser's bookmarking function.

The next time you want to start Host On-Demand, use the bookmark you created. The session starts without having to logon.



Anyone with access to your workstation can use the bookmark you created to logon to Host On-Demand with your ID.

Creating a bookmark that automatically starts a session

1. Start the Host On-Demand client you want to bookmark.
2. At the logon window, enter your user ID and password, then click Log On.
3. Right-click the icon for the session that you want to autostart with a bookmark.
4. Click **Set Up Bookmark**.
5. Select whether your session is to run in a separate window or in an HTML page within the browser window.

Choose **Run in a window** to run the Host On-Demand session in a window separate from your browser. This means that you can move and re-size the session window independently of the browser window and that the host session remains visible if you browse other Web sites.

Choose **Run in an HTML page** to run the Host On-Demand session as an HTML page embedded in your browser window. This means that the host session runs within the browser window and that you cannot move or resize it independently. If you browse another site, the session remains active but you cannot see it until you return to it (with the browser's Back button). Sessions bookmarked as Run in an HTML page do not have a menu bar.

6. The session starts. When prompted, bookmark the page.

The next time you want to start Host On-Demand, use the bookmark you created.



- The bookmark is based on the session name. If you change the session name or delete the icon for the session after you have created a bookmark, the bookmark will not work.
- Anyone with access to your workstation can use the bookmark to log on to Host On-Demand with your ID.

Creating a desktop icon for a bookmarked session

1. Create a desktop icon from your Host On-Demand bookmark by dragging and dropping the bookmark onto your desktop (not all browsers have this capability).
2. Double-click the Host On-Demand desktop icon to start a session.

Your browser probably lets you select it as your default browser. If you create a desktop icon with that browser, and later make another browser the default, the icon you created to start Host On-Demand may not work.

Bookmarking limitations

Locally-installed clients

You cannot use bookmarks to launch sessions on locally-installed clients.

Browser access

When creating bookmarks to launch sessions, Host On-Demand assumes that access to the browser is secure. If a browser contains a bookmark that bypasses the logon process, any person with access to the browser can use that bookmark to access Host On-Demand.

Error 501

Some Web servers do not support Host On-Demand's bookmarking feature. When you attempt to load a client from one of these servers, the following message appears: *Error 501 (Sorry, this server does not perform searches)*.

This problem has been observed on the following Web servers:

- Lotus Domino 4.5 on Windows NT
- IBM Internet Connection Server 4.x on iSeries

To avoid this problem, edit the client HTML file (HOD.html, for example) and add the following parameter:

```
<param name=bookmarking value="false">
```

Although the client will now load properly, users will not be able to use the bookmarking feature for their sessions.

If you are using the cached client, the procedure for disabling the bookmarking feature is different from that used with other clients. To disable bookmarking, do the following:

1. Edit the HTML file for the cached client (such as HODCached.html, for the English version or HOD.html).
2. Search for the following string:

```
var enableBookmarking = true;
```

3. Change the line as follows:

```
var enableBookmarking = false;
```

Bookmarks and multiple users

If more than one user creates bookmarks with the same browser, users cannot switch between the bookmarked sessions without closing the browser and restarting it. If a user logs on with a bookmark and then attempts to load another user's bookmark, the client will not load properly. To avoid this problem, log off, close the browser, and then restart it if you want to log on again using another user's bookmark.

Jump to next session

On a session window, click File > JumpNext to switch to the next session.

JumpNext and the jump key do not work on UNIX platforms with Netscape 4 because of Java Virtual Machines (JVM) limitations.

Java Virtual Machines that do not support the WINDOW_ICONIFY and WINDOW_DEICONIFY events may not jump correctly if the session you are jumping to is minimized.

Cutting, copying, and pasting in the Client window

[Marking and unmarking](#)

[Cutting](#)

[Copying](#)

[Pasting](#)

Marking and unmarking

Using your mouse

To mark a portion of text using a trim-rectangle:

1. Move the mouse pointer to one corner of the area you want to mark.
2. Click the left mouse button and drag the mouse diagonally until the area you want to mark is enclosed in a box.
3. Release the mouse button.

To move the trim-rectangle:

1. Move the mouse pointer into the marked area.
2. Click the left mouse button, drag the box, and release when the box is in the new location.

To unmark an area, click the left mouse button outside of the marked area, or click Edit > Unmark. Unmark is available only if text has been previously marked with a trim-rectangle.

Using your keyboard

To mark a portion of text using a trim-rectangle:

1. Move the cursor to one corner of the area you want to mark.
2. Press and hold Shift and use the cursor-movement keys (arrows) to mark the area.
3. Release Shift.

To mark the entire workstation window, click Edit > Select All.

To move the trim-rectangle:

1. Press and hold Ctrl.
2. Use the cursor-movement keys (arrows) to move the box to the desired location.
3. Release Ctrl.

To unmark an area, click Edit > Unmark.

Cutting

To cut the [marked text](#) into the clipboard:

- Click Edit > Cut.
or
- Press the key combination that is assigned to the Cut function. The default key combination is Shift + Delete.

You can set your preferences to support the cut function. It works similarly to the cut function in Personal Communications.

1. Click Edit > Preferences > Edit...
2. Click the preferences you want to set.
3. Click OK when you are finished.

If no area is marked, Cut copies the entire window and clears all unprotected fields, unless the [Cut/Copy only if a trim-rectangle is marked](#) function is enabled. Cut does not remove areas protected by the host application program. Cut does not duplicate host attributes, such as color or intensity.

Copying

To copy the [marked text](#) into the clipboard:

- Click Edit > Copy.
or
- Press the key combination that is assigned to the Copy function. The default key combination is Ctrl + Insert.

To append text that you have already copied into the clipboard:

- Click Edit > Copy Append.
or
- Press the key combination that is assigned to the Copy Append function. If your administrator has not already assigned a default key combination for this function, you can [assign a key combination](#) yourself.

To copy text into the clipboard that you want to place into columns in other applications, such as a spreadsheet:

- Click Edit > Copy as Table.
or
- Press the key combination that is assigned to the Copy as Table function. If your administrator has not already assigned a default key combination for this function, you can [assign a key combination](#) yourself.



The Copy as Table function formats text into columns by inserting a Tab character between columns and a New Line character at the end of every line. When using this function to copy columns of text into the clipboard, be sure to mark only text on the host screen that is formatted into columns. If you mark any text that is not formatted into columns, none of the text will format into columns when you [paste](#) it into another application.

We recommend that you do not use the Copy as Table and Copy Append functions when performing the same task.

You can set your preferences to support the advanced cut, copy, and paste functions. These functions work similarly to the cut, copy, and paste functions in Personal Communications.

1. Click Edit > Preferences > Edit....
2. Click the preferences you want to set.
3. Click OK when you are finished.

Copy duplicates the marked area into the clipboard without removing the marked area from the window. If no area is marked, Copy duplicates the entire window, unless the [Cut/Copy only if a trim-rectangle is marked](#) function is enabled. Copy does not duplicate host attributes, such as color or intensity.

Pasting

To paste text from the clipboard into your session at the current cursor position:

- Click Edit > Paste.
or
- Press the key combination that is assigned to the Paste function. The default key combination is Shift + Insert.

You can set your preferences to support the paste function. It works similarly to the paste function in Personal Communications.

1. Click Edit > Preferences > Edit....
 2. Click the preferences you want to set.
 3. Click OK when you are finished.
- If the data on the clipboard is larger than the space available, the data that doesn't fit is lost.
 - Paste does not overlay the clipboard contents onto areas that are protected by the host application.

- All text is pasted in the same rectangular shape used when it was copied or cut, unless the [Advanced paste function](#) is set.
- Text will not wrap, unless the [Advanced paste function](#) is set.
- Paste is not available if no data has been cut or copied to the clipboard.

Related topics

- [Using the keyboard to draw and move the trim box](#)
- [Cut/Copy tab](#)
- [Paste tab](#)
- [Trim tab](#)

Changing the current host session colors

To change the current host session colors, you can change the color settings. See [Understanding session colors](#) for an explanation of these color settings.

1. Click the button on the toolbar for "Set up display colors".
2. Click the area in the host session window of which you want to change the color. The color of the selected area appears in the Sample box.
3. To select a new color, either foreground or background, click the desired color in the color bar. The new color appears on the host screen immediately. To change to an exact color, click the Foreground Color or Background Color buttons to set RGB (red, green, and blue) values.
4. Click OK to accept changes made and return to the session. Click Cancel to cancel all changes and return to the session. Click Undo to undo the most recent change. Clicking Undo repeatedly will undo all recent changes in the order they were made, up to the point of when changes were started. Click Default to overwrite the profile customized colors with the program default colors. The Default button changes can be undone with the Undo button.

Changing colors using the Advanced color settings

If you are familiar with host screen elements and categories, you can change the color of a screen element using Advanced color settings.



Use this method to change the color of elements in the operator information area (OIA) because these elements cannot be changed by clicking the appropriate area on the OIA region.

To use Advanced color settings to change the colors of screen elements:

1. Click the button on the toolbar for "Set up display colors".
2. Click the Advanced button.
3. Select the category and element you want to change. The color mapped to that category and element appears in the Sample box.

The available categories and elements are listed under [3270 elements](#), [5250 elements](#), and [VT elements](#). The available OIA elements are the same for all session types and are listed under [Operator Information Area elements](#).

If the color in the Sample box is different than the color in the Element list, then the color for that area has already been remapped. You can remap these again.

4. To select a new color, click the desired color in the color bar. To change to an exact color, click the Foreground Color or Background Color buttons to set RGB (red, green, and blue) values.
5. Click OK to accept changes made and return to the session. Click Cancel to cancel all changes and return to the session. Click Undo to undo the most recent change. Clicking Undo repeatedly will undo all recent changes in the order they were made, up to the point of when changes were started. Click Default to overwrite the profile customized colors to the program default colors. The Default button changes can be undone with the Undo button.
 - Other users cannot use your remapped colors. Color mapping is saved with the icon that launched the session in your account-file (HOD.[your_id].user) on the server from which the session was loaded.
 - You can use the remapped colors with every session you launch from the same icon but not with sessions launched from other icons (unless they are copies of the original session made after the colors were remapped).



3270 elements

For 3270 sessions, you can define these elements.

The base attributes include:

- Normal, unprotected
- Intensified, unprotected
- Normal, protected
- Intensified, protected

The extended attributes include:

- Blue
- Green
- Pink
- Red
- Turquoise
- White
- Yellow
- Default intensified

The graphics attributes include:

- Default
- Blue
- Red
- Pink
- Green
- Turquoise
- Yellow
- White
- Black
- Dark Brown
- Orange
- Purple
- Dark Green
- Dark Turquoise
- Mustard
- Grey
- Brown

The OIA color elements are defined in [Operator Information Area elements](#).

5250 elements

For 5250 sessions, you can define these elements.

The field color attributes include:

- Green

- White
- Red
- Turquoise
- Pink
- Blue
- Yellow
- Status indicators

The OIA color elements are defined in [Operator Information Area elements](#).

VT elements

For VT sessions, you can define colors within the following categories: Base color, ANSI attributes, and OIA color.

The following elements are available in the Base color category:

- Normal
- Bold
- History Normal
- History Bold

The following elements are available in the ANSI attributes:

- Blue
- Green
- Pink
- Red
- Turquoise
- White
- Yellow

The OIA color elements are defined in [Operator Information Area elements](#).

Operator Information Area elements

The OIA color refers to the operator information area (OIA) on the bottom row of the host session window. There are several types of information that might appear on this row, and you can change the color for each. The OIA attributes are the same for all session types.

- Status indicators (readiness, system connection, shift and modes, and insert-mode) inform you of the current terminal status.
- Information indicators (system lock and wait, which is the clock symbol) appear infrequently and do not require any particular action from you.
- Attention indicators (machine check, communication check, and program check) indicate unpredictable situations that occur from time to time in response to operator or system actions.
- Error indicators (what?, wrong place, too much data, numeric data only, what number?, minus function, operator not authorized, minus symbol, and rejected message) indicate conditions that the system regards as erroneous and occur whenever a given action has been made in a given circumstance.
- OIA background

Related tasks

- [Understanding session colors](#)
- [Using the host session default colors](#)

Cut/Copy tab



You can set your preferences to support the Cut/Copy functions. These functions work similarly to the Cut/Copy functions in Personal Communications.

Cut/Copy only if a trim-rectangle is marked

Disables the Edit > Copy, Edit > Copy Append, Edit > Copy as Table, and Edit > Cut functions until you draw a [trim-rectangle](#) or until you use the keyboard to select a block of text. In other words, if you check this box, you must draw a trim-rectangle in order to use the cut or copy functions.

If you leave the checkbox unchecked, the Edit > Copy, Edit > Copy Append, Edit > Copy as Table, and Edit > Cut functions cut or copy the entire screen if no trim-rectangle is drawn, or the contents of a trim-rectangle, if one is drawn.

Important:

The following JVM environments do not set the clipboard correctly and may produce copy and paste results that are not accurate:

- Netscape JDK 1.1.5
- Netscape JDK 1.1.6

Related topics

- [Cutting, copying and pasting in the Client window](#)
- [Using the keyboard to draw and move the trim box](#)

Paste tab



You can set your preferences to support the paste function, which works similarly to the paste function in Personal Communications.

Field Wrap

Allows the data that would fall onto a protected field to be pushed into the nearest following unprotected field. The Field Wrap function does not break words in the middle, except when the first word encounters a protected field. For example, if you try to paste the phrase *Host On-Demand* into an eight-character unprotected field, the function pastes *Host* in that field and pastes *On-Demand* in the next unprotected field that can accommodate the remaining nine characters. However, if you try to paste the phrase *Host On-Demand* into an unprotected field of 20 characters where only the character in the second position is protected, the function pastes the phrase like this: *H ost On-Demand*.

If you leave the checkbox unchecked, any data that falls on a protected field is lost.

Line Wrap

Enables the Line Wrap function to recognize end-of-line and end-of-screen indicators and continue to paste your data. When an end-of-screen indicator is encountered, the Edit > Paste Next menu item is enabled for you to paste the remaining text. Data that falls on a protected field is lost, unless the Field Wrap function is enabled. If the data you are pasting breaks in the middle of a word, enable the Field Wrap function to keep words intact.

If you leave the checkbox unchecked, any data that doesn't fit in the specified unprotected field is lost.

Paste to marked area

Determines if you use a trim-rectangle to designate exactly where to paste your data.

If you leave the checkbox unchecked, the Paste and Paste Next functions paste your data where the cursor is (not at the trim-rectangle).

Stop pasting when protected field encountered

Allows your data to be pasted until a protected field is encountered. The Edit > Paste Next function allows you to paste the remaining text in an unprotected field.

If you leave the checkbox unchecked, any data that falls on a protected field is lost, unless the Field Wrap function is enabled.

Tab character processing

These paste preferences indicate how tab characters should be processed when pasting.

Advance to next tab stop

Enables you to align tabulated text at specified tab stops. For example, if you click the Advance to next tab stop radio button and you indicate 10 in the column(s) per tab stop field, your tabulated text is pushed to the column position that is the next multiple of 10.

Replace with:

Allows you to replace tab stops with a specified number of spaces. For example, if you click the Replace with: radio button and you indicate 3 in the space(s) field, each tab stop in your original text becomes 3 spaces.

Paste data to fields (for 5250 sessions only)

Determines whether your tabulated text is placed in subsequent unprotected fields. When a tab character is encountered, the following text data is pasted into the next unprotected field on the same line of the emulator

session.

Important:

The following JVM environments do not set the clipboard correctly and may produce copy and paste results that are not accurate:

- Netscape JDK 1.1.5
- Netscape JDK 1.1.6

Related topics

- [Cutting, copying and pasting in a client window](#)
- [Using the keyboard to draw and move the trim box](#)

Using the keyboard to draw and move the trim box

Use these key combinations to draw a trim box.

Key combination	Description
Shift+Up arrow	Mark box up
Shift+Down arrow	Mark box down
Shift+Left arrow	Mark box left
Shift+Right arrow	Mark box right
Shift+Esc	Remove box from screen

Use these key combinations to move a trim box.

Key combination	Description
Ctrl+Up arrow	Move box up
Ctrl+Down arrow	Move box down
Ctrl+Left arrow	Move box left
Ctrl+Right arrow	Move box right

Related topics

- [Marking and unmarking](#)

Trim tab

You can set your preferences to support the Cut/Copy, and Paste functions. These functions work similarly to the Cut/Copy and Paste functions in Personal Communications.

Trim Rectangle sizing handles

Allows you to resize a trim-rectangle after you draw it using any of the eight handles around its perimeter. If you put the mouse cursor on one of these handles, the mouse cursor changes to a double-headed arrow, indicating that you can click-and-drag the handle either direction to resize the trim-rectangle.

If you leave the checkbox unchecked, the trim-rectangle is not resizeable, but you can draw new trim-rectangles until you have the size you want.

Trim Rectangle remains after edit function

Enables the trim-rectangle to remain on the screen after you complete your cut or copy. You can then drag the rectangle to another location on the screen if you want to paste into an area of exactly the same size.

If you leave the checkbox unchecked, the trim-rectangle disappears when you complete your [cut or copy](#) function.

Important:

The following JVM environments do not set the clipboard correctly and may produce copy and paste results that are not accurate:

- Netscape JDK 1.1.5
- Netscape JDK 1.1.6

Related topics

- [Cutting, copying and pasting in the client window](#)
- [Using the keyboard to draw and move the trim box](#)

Understanding session colors



Each host screen is made up of fields with attributes. Elements are simply a way to group fields that share the same type of 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. That is because those fields are the same element (they share the same attributes) as the field for which you remapped the color. Some other fields that were the original color will not be changed, as you might expect. That is because those fields are not the same element (they do not share the same attributes) as the field for which you remapped the color. You can remap these original-colored fields the same way you remapped the other fields.

For example, if an input field is white and you remap the color to yellow, other input fields may appear yellow instead of white as well. However, some input fields may remain white. You can remap these to yellow as well.

Advanced settings

We recommend you only use the advanced settings method if you are familiar with host fields, elements, and attributes. Advanced settings lets you remap the color of all the fields that are the same element (share the same attributes), just like the basic settings. However, instead of clicking in the field you want to change on the screen, you can specify the element you want to change throughout your host applications. Even in advanced settings, you can still click on the screen to change the color, but the advanced-setting method is primarily for you to remap by element.

For example, if a normal, unprotected field uses white text, you can change the color of all normal, unprotected fields to yellow.

Related tasks

- [Changing the current host session colors](#)
- [Using the host session default colors](#)

Resetting the host session default colors

To return to the default colors defined by the host application:

1. Click the button on the toolbar for "Set up display colors" or select Edit > Preferences > Color....
2. Click Default.
3. Click OK. The Default button changes can be undone with the Undo button.

Printing a screen



To print a terminal emulator session screen, click File > Print screen.

You can only print screens to printers installed on your desktop.

Before printing a screen, you can optionally set the following printing parameters:

- To specify the page orientation, paper source, and margins, click File > Print Screen Setup > Page Setup.
- To add headers and footers to your printout and suppress the Print window, click File > Print Screen Setup > Print Setup.



The Page Setup and Print Setup commands are available only on browsers that support Java 2.

You can print the entire presentation space of your Host On-Demand window when there is no marked area using a trim-rectangle. If there is a marked area, only that portion of the presentation space is printed out. To print the entire presentation space even when there is a marked area, you can do it by setting the `markedAreaPrintingEnabled` HTML parameter to `false` in your client HTML page. For example, set:

```
<PARAM NAME=markedAreaPrintingEnabled VALUE=false>.
```

The default value is `true`.

When you print a host graphics screen, the image is scaled to print on paper; therefore, print quality may be degraded.

If the Host On-Demand Print Screen menu and toolbar option does not work on your Unix system when the output is directed to a printer, you can do the following:

1. Select Print Screen from the menu bar or tool bar of the session
2. Select to the send the output to FILE and enter a file name
3. Use the Unix LPR command to send the file to a network printer. The command syntax is:

```
LPR -Pprinterqueue filename
```

For example,

```
LPR -P51pcl /home/usr.txt
```



The Print Screen function does not work on the AIX platform due to a browser JVM problem on AIX.

The Print Screen function of Host On-Demand uses a programming interface provided by Java. It works on most platforms, but it does not work on some Unix-based operating systems, such as Linux. The implementation of the programming interface uses the Unix `lp` command, which is not available on some Unix-based operating systems.

Following is the workaround for this problem:

1. Log into the system as a superuser.
2. Open a terminal session to input commands from prompt.
3. Change directory to the directory where `lpr` command is stored. Typically, it is `/usr/bin`. If this is so, type

```
cd /usr/bin
```

4. Create a symbolic link with the `ln` command. Type


```
ln -s lpr lp
```


5. Log out.
6. Log in to the system as a user and start a Host On-Demand display session.
7. Click File > Print Screen.
8. Delete the string specified for Banner Page Title. By default, it is specified like Print Screen.
9. Press OK.

Related topics:

- [Page Setup window](#)
- [Print Setup window](#)

Page Setup window



 This window is available only on browsers that support Java 2.

Choose File > Print Screen Setup > Page Setup to modify the page layout for a printed screen.

Paper

Select the paper size and source:

Size

Select one of the paper sizes defined for the current default printer.

Source

Select one of the paper sources defined for the current default printer.

Orientation

Select one of the following page orientations:

Portrait

Prints the screen so that the short edge of the paper is the top of the image.

Landscape

Prints the screen so that the long edge of the paper is the top of the image.

Margins

Enter the width of the margins in the units given.

Top

The distance between the top edge of the paper and the top of the printed area.

Bottom

The distance between the bottom edge of the paper and the bottom of the printed area.


Left

The distance between the left edge of the paper and the left side of the printed area.

Right

The distance between the right edge of the paper and the right side of the printed area.

When you change the page orientation, the printer swaps the Top and Bottom margins with the Left and Right margins.

 Host On-Demand cannot set margins on the Linux platform due to a limitation in the Linux JDK.


Related topics:

- [Printing a screen](#)
- [Print Setup window](#)

Print Setup window



Choose File > Print Screen Setup > Print Setup to add headers and footers to terminal emulator screen printouts and suppress the display of the Print window.

 This window is available only on browsers that support Java 2.

Header

Lets you specify the text of a header that appears at the top margin of a printed screen.

Place

The horizontal alignment of the header. Can be one of the following:

Left

Aligned with the left margin.

Right


Aligned with the right margin

Centered

Centered between the left and right margins

Text

The header text. Headers can include automatically updated page numbers, dates, times, and so forth; see [Special header and footer characters](#) for a complete list.

 When Screen Customizer is enabled, the print preview function does not show header text.

Footer

Lets you specify the text of a footer that appears at the bottom margin of a printed screen.

Place

The horizontal alignment of the footer. Can be one of the following:

Left

Aligned with the left margin.

Right


Aligned with the right margin

Centered

Centered between the left and right margins

Text

The footer text. Footers can include automatically updated page numbers, dates, times, and so forth; see [Special header and footer characters](#) for a complete list.

 When Screen Customizer is enabled, the print preview function does not show footer text.

Special header and footer characters

A set of predefined special characters allows you to include times, dates, page numbers, and other characters in headers and footers.

Character	Printed as ...
&d or &D	The current date. The date format depends on your NLS locale. (For example, the date format for the en_US locale is dd-mmm-yy.)
&t or &T	The current time. The time format depends on your NLS locale. (For example, the date format for the en_US locale is hh:mm:ss AM/PM.)
&p or &P	The current page number.
&n or &N	The newline character. This is especially useful for creating space between the header and screen image.
&&	The ampersand (&) character.

Suppress print window when printing

Select Yes to suppress the display of the Print window when you print a screen. The Print window 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.

Printer button

Click this button to display the standard Print window for your platform. This button is enabled only in a running session.

Page Setup button

Click this button to display the [Page Setup](#) window, enabling you to specify the paper type, page orientation and margins for your printouts.

Related topics:

- [Printing a screen](#)
- [Page Setup window](#)

Changing certificate settings



Each certificate is encrypted with a password. To change the password:

1. Click Communication > Security.
2. Click Show Client Certificate.
3. Locate the certificate and type the current password.
4. Click View Certificate.
5. Click Settings.

Current Password

Type the current password for the selected certificate.

New Password

Type the new password for the selected certificate.

Confirm New Password

Type the new password again.

Encryption Strength

Strong or Weak

Certificates exported from older browsers are usually weakly encrypted. Certificates exported from newer browsers, Certificate Management, or Certificate Wizard are strongly encrypted. This makes them more secure from unauthorized access, but they cannot be imported into most older browsers. Use strong encryption when the certificate will be accessed over the Internet with an unsecure protocol, such as http or ftp. Certificates accessed using https, ftps, or from the local file system do not need to be strongly encrypted. Use weak encryption only when the certificate is not accessed with an unsecure protocol and must be imported into an older browser.

Related topics

- [Client authentication](#)



Viewing server certificate



information

To view server certificate information, click Communication > Security. When a secure connection has been attempted, the certificate is sent from the server. Even if the connection is not successful, the certificate may still be available to view. Select a field from the Field list box. The value for the selected field is displayed in the Value field. The server's certificate might not contain values for all the fields.

If you cannot complete a secure connection to the server, it may be because the server's certificate is not trusted by your client. In this case COMM662 will appear in the OIA of the emulator and error message ECL0009 will be logged. To complete the connection, you can extract the appropriate server certificate and add it to the list of trusted CAs. If Show Issuer Certificate is not grayed out, click that button to display the issuer of the server's certificate and extract the issuer's certificate to a file. If Show Issuer Certificate is grayed out, click Extract to save the server's certificate to a file. You can then [add it to the list of trusted CAs](#) (for locally-installed clients) or send it to your Host On-Demand administrator to add to the CustomizedCAs.class file on the server (for all other clients).



Certificates received over the Internet can be forged. The safest way to verify the authenticity of a certificate is to display the finger print of the certificate you have received, and then contact the administrator of the server you are connecting to and ask for the finger print of the certificate on the server. If the finger prints match, you have an authentic certificate and may safely add it to the list of trusted CAs.

Click Show Client Certificate to select and view a client certificate. This is a certificate file that was given to you by the person who requested and received your certificate.

Click Show CAs Trusted by the Client to see a list of CAs that the client can trust. These are the well-known CAs and the CAs listed in the CustomizedCAs.class file located on the Host On-Demand server for download clients or the Host On-Demand locally-installed client. If the session is configured with Add MSIE browser's keyring set to yes, then those trusted certificates will be displayed also.

Click Show Issuer Certificate to view information about the issuer of the requesting server's certificate, if it is available. This provides an additional security check because you can check that the certificate is signed by its expected CA.

You cannot view the server's certificate without attempting to connect to the server first. However, you can view your client certificates and see a list of CAs trusted by the client.

Related topics

- [Client authentication](#)

Viewing or saving client certificate information

1. Click Communication > Security.
2. Click Show Client Certificate.
3. Locate the certificate, enter the password, and click View Certificate.
4. Select a field from the Field list box. The value for the selected field is displayed in the Value field. Some values might not be available.

If the selected certificate is in a local file, the password or the encryption strength can be changed by clicking Settings

To view information about the issuer of the certificate if it's available, click Show Issuer Certificate.

To save the public information of the client certificate in a different format or location, click Extract. A server administrator might require you to do this step.

Related topic:

- [Client authentication](#)

National Language Support

You can select a language for each 3270, 5250, VT, or CICS session from the list of supported code pages in the session properties window.

Java National Language Support is platform-dependent, so you must install the appropriate font and keyboard support for your selected language on the underlying operating system. For example, if you select French for a session language, but do not have French font and keyboard support installed, you might not be able to display the correct French characters.

- [No monospaced fonts in Korean 5250 and 3270 sessions](#)
- [Adobe PDF default paper sizes](#)
- [Adobe PDF default fonts](#)
- [IBM Worldtype fonts](#)
- [Keys that do not work on the IME keypad for DBCS languages](#)
- [Arabic, Hebrew and Thai support with Netscape 4](#)
- [Character display with Netscape 4 for Windows \(European Languages\)](#)
- [Inputting Japanese Characters](#)
- [Greek-language limitation on scrolling Action Keys list box](#)
- [Generating SO/SI automatically](#)
- [Displaying a split DBCS character](#)
- [User-Defined Character \(UDC\) support](#)
- [Korean and Traditional Chinese with Netscape 4.06 on Windows NT, 95 and 98](#)
- [Simplified Chinese with Netscape 4.06](#)
- [Simplified Chinese on AIX](#)
- [IBM-Selected characters on AIX](#)
- [Japanese character-conversion through the clipboard](#)
- [SAA characters with Internet Explorer 4 and Netscape 4](#)
- [Korean - Incorrect font with Internet Explorer 4.0 on Windows NT](#)
- [Chinese \(Traditional\) - Incorrect font with Internet Explorer 4.0 on Windows NT](#)
- [Backslash displays as yen](#)
- [Restrictions on automatic shift change](#)
- [Restriction on cursor width](#)
- [Restriction on using DBCS code pages with the CICS-gateway emulator](#)
- [Restrictions on file transfer](#)
- [Restrictions on Japanese Unicode Extended code pages \(1390/1399\) support](#)
- [Restrictions on Taiwan and Korea code pages 1371/1364 support](#)
- [Restriction using "On the Spot Conversion" function with SUN Java2 Plugin 1.3](#)
- [Support for user-defined characters](#)
- [Font-size does not change on OS/2 - fix](#)
- [Euro dollar symbol copy and paste](#)
- [Print Screen when the marked area trim-rectangle contains split DBCS characters](#)
- [Some half-width characters cannot be displayed in a TSO environment](#)
- [Korean DBCS with Netscape 4.7.2 on AIX](#)

- [Print Screen on Windows 2000 in a session using monospaced fonts](#)
- [Corrupted National language characters in text entry fields](#)
- [Selection box appears to truncate top lines on AIX with Netscape DBCS](#)
- [DBCS filenames and paths are not displayed for Netscape on AIX](#)
- [Some DBCS characters appear with '{?}' on T,P,J,K-OS/2 4.0 Merlin](#)
- [DBCS input field's character can't output to other fields on Netscape for AIX](#)
- [DBCS Gaiji mapping table](#)
- [DBCS GB18030 support](#)
- [Scroll bar does not work normally on Netscape 4.61 with JDK1.1.8 for OS/2 platform](#)
- [Last interim Hangeul is not displayed](#)
- [Korean "Won" and Japanese "Yen" appear as backslashes \(\\) on Korean and Japanese Win32 browsers](#)
- [The IME toolbar mistakenly turns on when clicking sessions using Java 2](#)
- [On-the-spot conversion](#)
- [Auto IME function does not work on any DBCS version of Linux](#)
- [Auto IME function with Simplified and Traditional Chinese](#)
- [IME toolbar disappears on Simplified Chinese OS/2 Warp 4 with IBM Java2 Plugin](#)
- [Auto IME function on Korean Windows](#)

No monospaced fonts in Korean 5250 and 3270 sessions

To avoid this problem on Microsoft Internet Explorer, edit the Windows registry.

1. Type regedit on the command line.
2. Click HKEY_LOCAL_MACHINE > SOFTWARE > MICROSOFT > Java VM > Font Alias.
3. In the Edit String window, change Courier to the Korean font (GulLimChe: 3 Korean characters).
4. Click OK.

Adobe PDF default paper sizes

The default paper size for US English and Canadian locales is Letter. For all other locales, the default paper size is A4.

Adobe PDF default fonts

For non-DBCS, non-Bidi, non-Thai languages (i.e. all European languages except for Greek, Latin 2, and Baltic languages), the default font is Courier.

For Greek, Latin 2, and Baltic languages, the default font is CourierNewPSMT. This is because the Courier font provided with Host On-Demand does not have certain characters used in those languages.

For DBCS, Bidi, or Thai languages, see the following table:

Language	Default font
Simplified Chinese	STSongStd-Light-Acro
Traditional Chinese	MSungStd-Light-Acro
Korean	HYSMyeongJoStd-Medium-Acro

Japanese	KozMinPro-Regular-Acro
Thai	Courier Thai
Arabic	Typing Arabic
Hebrew	Cumberland

Both LucidaConsole and CourierNewPSMT fonts correspond to the Courier New and Lucida Console fonts that are commonly available on Windows platforms. In order for Adobe PDF files to properly display these two fonts, users will need newer versions of the Windows platform, such as Windows 98 Second Edition, Windows ME, Windows 2000, or Windows XP.

IBM Worldtype fonts

With the release of the Developer Kit for Linux, IBM offers additional font packages. The font packages provide additional double-byte character set (DBCS) support. The font packages are provided because Java is able to display all Unicode characters, but most versions of Linux install only the fonts needed to display the country- or region-specific font. The font packages do not replace the system fonts. These fonts are currently available on the Host On-Demand Support page at <http://www.ibm.com/software/webervers/hostondemand/support.html>.

Monotype Sans Duospace WorldType fonts		
Font	File name	Country/region
Monotype Sans Duospace WTJ	mtsansdj.ttf	Japan and other countries
Monotype Sans Duospace WTTK	mtsansdk.ttf	Korea
Monotype Sans Duospace WTSC	mtsansds.ttf	China (Simplified Chinese)
Monotype Sans Duospace WTTC	mtsansdt.ttf	Taiwan (Traditional Chinese)

Keys that do not work on the IME keypad for DBCS languages

The Backspace, Tab and Enter keys on the IME keypad do not work.

Arabic, Hebrew and Thai support with Netscape 4

If you are using Netscape 4 and JVM 1.1.5 or lower, Arabic, Hebrew and Thai characters do not display if you use the Courier or Monospaced fonts, and Print Screen does not work. If you install the appropriate raster font set (ARB3270, HEB3270, THA3270) and select it on the Screen page of the session configuration, characters will display, though Print Screen may still not work.

Character display with Netscape 4 for Windows (European Languages)

With Netscape 4, it is not possible to display correctly the characters of some European languages, such as Turkish, Russian, Hungarian, Polish, Slovenian, Czech or Greek. This is because of a deficiency in the JVM.

To solve this problem, sample font-properties files are provided in the `hostondemand\hod\samples\fonts\win32` directory; you should copy the appropriate files into your `netscape\communicator\program\java\classes` directory (after packing up the original files).

Inputting Japanese characters

If you want to enter Japanese characters, press the double-byte character set (DBCS) input key. A text field displays. You can type any Japanese or alphanumeric characters into this text field using the Input Method provided by your operating system. You can also use any Host On-Demand key functions in this text field. you do not need to close the window to perform another session operation.

To close the window, press the DBCS Input key again.

When you close this window, make sure you exit the Input Method you used to input the Japanese characters. If you do not exit the Input Method, you might not be able to type characters on the session screen.

Some browsers, such as Internet Explorer 4.0x and Netscape Communicator 4.0x, support the Japanese character input method to type characters into a Host On-Demand window. In this case, you don't need to use the Japanese Input dialog box.

Greek-language limitation on scrolling Action Keys list box

Users who are using Host On-Demand using Internet Explorer on a Greek personal computer running Windows 98 cannot scroll down the Action Keys list box in the Host On-Demand Macro Editor. To locate this list box, use the following path: View > Macro Manager > Host Access Macro Editor > Screens > Actions.

Generating SO/SI automatically

When you input DBCS characters in a 3270 or 5250 session, a Shift Out (SO) character must be inserted where the DBCS characters begin and a Shift In (SI) character must be inserted where the DBCS characters end.

Host On-Demand automatically generates SO/SI characters where they are required. When your cursor is at the first position of the 5250 DBCS Either field and you type a DBCS character, the field automatically becomes a DBCS character-enabled field, and will accept only DBCS characters. If you type an SBCS character in the first position of a field, the field automatically becomes an SBCS character-enabled field and will accept only SBCS (alphanumeric) characters.

Displaying a split DBCS character

When a DBCS character is split between two lines, half the character displays at the right end of the line and a special symbol displays at the left end of the next line.

User-Defined Character (UDC) support

[User-defined characters for host-printing sessions](#)

[User-defined characters for display sessions](#)

User-defined characters for host-printing sessions

For Host Printing support of User-Defined Characters (UDCs), you must prepare a UDC font-image file. On a server, this file must be located in the `\ondemand\hod\fonts\` directory for access by clients. On a locally-installed client, the file must be located in the `\ondemand\lib\fonts` directory.

On Windows 95, 98 or NT, you must run the **w32udcnv.exe** utility to 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 or client during installation. To use the utility:

1. 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:

0

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 `\ondemand\hod(or lib)\fonts` directory.

On an OS/2 server, copy the OS/2 font-image file, `$SYS1Z24.FNT`, to the `\ondemand\hod\fonts` directory and rename it according to the table above.

Unicode Support of UDCs (Japan only)

On Japanese Windows 2000, a unicode version utility, `w32udcnvw.exe`, is provided to convert Windows user-defined fonts into a usable font-image file. If you use this utility to convert the UDCs on Windows 2000, all the UDCs defined by unicode are converted. Host On-Demand can print not only the UDCs defined in PC codes (totally 1880 characters), but also those defined in unicode including the host UDCs (0x6941-0x89BD for 930/939, 0x6941-0x7FFE for 1390/1399).

Limitations

- In a Traditional Chinese Windows environment, there are 13 more UDCs than IBM's Big5 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.

User-defined characters for display sessions

JAVA 1.1x does not support the display or input of user-defined characters; however, with some browsers, there is a workaround. Internet Explorer 4.0 for Windows 95, 98 or NT has its own workaround. With Netscape 4.0x for Windows and HotJava 1.x for Windows, you must change the font-property file provided by the browsers to register a class for character-set conversion. For details, please refer to the files in the `\samples\fonts\dbc_s_udc` directory on the Host On-Demand CD; this contains a sample class for character-set conversion, a sample font-property file, and instructions.

Korean and Traditional Chinese with Netscape 4.06 on Windows NT, 95 and 98

[Korean](#)
[Traditional Chinese](#)

On Korean and Traditional-Chinese Windows 95 and NT, with Netscape 4.06, some characters may not be displayed in the host-session screen at all, or the wrong characters are displayed and the screen looks corrupted. This happens because the font used to display characters is not selected correctly, probably because the font-properties file is incorrect.

You might be able to solve this problem by installing the latest version of Netscape 4.06; if not, workarounds are available as follows:

Korean

- Go to Netscape's `\program\java\classes` directory.
- Back up the `font.properties.ko` file.
- Modify the file as follows to change the definitions for the Monospaced font from:

```
monospaced.0=Gulim,HANGEUL_CHARSET
monospaced.1=Courier New,ANSI_CHARSET
monospaced.2=WingDings,SYMBOL_CHARSET,NEED_CONVERTED
monospaced.3=Symbol,SYMBOL_CHARSET,NEED_CONVERTED
to
monospaced.0=\uad74\u9bc\uccb4,HANGEUL_CHARSET
monospaced.1=Courier New,ANSI_CHARSET
monospaced.2=WingDings,SYMBOL_CHARSET,NEED_CONVERTED
monospaced.3=Symbol,SYMBOL_CHARSET,NEED_CONVERTED
```

Traditional Chinese

1. Go to Netscape's \program\java\classes directory.
2. Back up the font.properties.zh_TW file.
3. Modify the file as follows to change the definitions for the Monospaced font from:

```
monospaced.0=\u7d30\u660e\u9ad4,CHINESEBIG5_CHARSET,NEED_CONVERTED
monospaced.1=Courier New,ANSI_CHARSET
to:
monospaced.0=Courier New,ANSI_CHARSET
monospaced.1=\u7d30\u660e\u9ad4,CHINESEBIG5_CHARSET,NEED_CONVERTED
```

and change:

```
fontcharset.monospaced.0=sun.io.CharToByteBig5
to:
fontcharset.monospaced.1=sun.io.CharToByteBig5
```

and change:

```
exclusion.monospaced.1=0100-f8ff
to:
exclusion.monospaced.0=0100-f8ff
```

If these workarounds do not work completely:

1. Back up the font.properties.ko or font.properties.zh_TW files.
2. Copy the font-property files from Sun's JDK 1.1.5 to Netscape's program\java\classes directory.
Note: do **not** use the files from the JDK 1.1.6.

Even with the 1.1.5 JDK, the broken-bar SAA character does not display.

Simplified Chinese with Netscape 4.06

On Simplified-Chinese Windows 95 and NT with Netscape 4.06, you may not be able to type the correct Chinese characters when using the Input Method Editor (the IME lets you input double-byte characters in addition to alphanumeric characters). You might be able to solve this problem by installing the latest version of Netscape 4.06.

Simplified Chinese on AIX

You cannot enter Simplified Chinese characters onto a host-session screen on AIX.

IBM-Selected characters on AIX

On AIX (Japanese EUC or 932), with host code-pages 930 and 939, IBM-Selected characters cannot be displayed correctly.

Japanese character-conversion through the clipboard

On Japanese Windows NT 4.0, 95 and 98, with host code-pages 930 and 939, when host code-points X'41F2'-X'41FA' and X'446D'-X'446F' are copied through the clipboard, they are always converted to NEC-Selected characters, not IBM-Selected.

SAA characters with Internet Explorer 4 and Netscape 4

SAA characters (characters that exist in host code-pages but not in PC code-pages) are not defined in DBCS fonts (for example, Gothic, gulimche, simiti), and cannot be displayed correctly with Microsoft Internet Explorer. Some Japanese examples are (X'xx' is in EBCDIC):

```
X'4A':Cent  
X'5F':Logical Not  
X'A0':Over-bar  
X'B1':UK Pound  
X'E0':Backslash
```

The SAA characters Cent, LogicalNot, and Pound sign do not copy and paste correctly using Netscape 4.x on the DBCS version of Microsoft Windows 95/98/ME and OS/2. These SAA characters will become DBCS and appear incorrectly if they are copied and pasted.

Korean - Incorrect font with Internet Explorer 4.0 on Windows NT

Microsoft Internet Explorer 4.0 does not specify the correct font for Korean. You can fix this by replacing the data for the Courier font with **Gulimche** (written in Korean) in the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM\Font Alias\Courier
```

Chinese (Traditional) - Incorrect font with Internet Explorer 4.0 on Windows NT

Microsoft Internet Explorer 4.0 does not specify the correct font for Chinese. You can fix this by replacing the data for the Courier font with **simiti** (written in Chinese) in the following registry entry:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM\Font Alias\Courier

Backslash displays as yen

If you type a backslash with either a US 101-key or Japanese 106-key keyboard on Japanese Windows NT, 95 or 98, it displays as a Yen sign. This seems to be a problem with both Netscape 4 and Internet Explorer 4.

Restrictions

[Automatic shift change](#)

[Cursor width](#)

[Using DBCS code pages with the CICS gateway emulator](#)

[File transfer](#)

Restrictions on automatic shift change

Host On-Demand does not support the following functions because of JAVA 1.1.x restrictions on controlling the shift status or IME status:

1. Automatic shift-status change when the cursor enters or exits a DBCS-enabled field
2. Automatic shift-status change when the cursor enters or exits a 5250 Katakana shift field

You must therefore change the shift or IME status manually to input characters in a particular shift status.

Restriction on cursor width

Host On-Demand does not support changing the cursor width automatically when the cursor is positioned under DBCS characters. The cursor width always stays the same.

Restrictions on using DBCS code pages with the CICS-gateway emulator

Host On-Demand does not support DBCS code-pages with the CICS-gateway emulator.

Restrictions on file transfer

The following DBCS code-pages are supported by Host On-Demand file transfer. Note that some characters extended by the respective operating system cannot be shown or converted correctly.

Korea - IBM KS code (code page IBM-949)

Does not support Hangeul characters extended by Microsoft (code page MS-949)

S-Chinese - IBM GB code (code page IBM-1381)

Does not support characters extended by GBK (code page MS-936)

T-Chinese - IBM Big5 code (code page IBM-950)

Does not support some vendor-defined and user-defined characters

Restrictions on Japanese Unicode Extended code pages (1390/1399) support

The following restrictions apply to Japanese Unicode Extended code pages (1390 - Katakana Unicode Extended / 1399 - Latin

Unicode Extended) support:

- 1390 code page is supported only on 3270 sessions.
- Because Windows 95 does not support Unicode, most of the new DBCS code points provided in the Japanese host (EBCDIC) code pages 1390/1399 are not supported.
- DBCS host code points (not found in PC code page 943 (=MS932)) can not be entered using Input Method Editor (IME) provided with Windows NT, Windows 98, and Windows 2000. You can enter them using the Unicode character table (ucharmap.exe) that comes with Windows NT and Windows 2000. However, Windows 98 does not provide ucharmap.exe.
- The new DBCS User Defined Font area (not found in PC code page 943 (=MS932)) can be defined only by the User Defined Character Editor (eudcredit.exe) in Windows 2000. The User Defined Character Editor in Windows 98 or Windows NT does not support code points in Unicode.
- On Windows 2000, two User Defined Characters (X'7EAC' and X'7EAD' on host code pages; U+F001 and U+F002 on Unicode) are already used by Windows. You cannot override these characters.
- The Japanese host code pages 1390/1399 contain many characters that are not found in Japanese ASCII code pages. Some characters, including Euro dollar symbol, are not displayed correctly on Windows NT, Windows 98, and Windows 2000 due to the restrictions of Windows fonts.

Restrictions on Taiwan and Korea code pages 1371/1364 support

In the Taiwan and Korea host code pages 1371/1364, Euro sign can not be displayed correctly on Windows NT, Windows 98, and Windows 2000 due to the restrictions of fonts in Windows.

In the Taiwan host code page 1371, single byte character set (SBCS) and double byte character set (DBCS) Euro signs are displayed as the same size because only one unicode of Euro sign is defined.

Restriction using "On the Spot Conversion" function with SUN Java2 Plugin 1.3

You must use SUN Java2 Plugin 1.3 with the "On the Spot Conversion" function. If you do not use SUN Java2 Plugin 1.3, a NullPointerException will be displayed on the Java Console.

Support for user-defined characters

JVMs do not currently support the display or input of user-defined characters; however, there are workarounds.

Internet Explorer 4.0 for Windows 98 and Windows NT has its own workaround. Use the Gaiji editor to create user-defined characters. (Click Start > Programs > Accessories to access the editor.) The workaround does not work for Windows 95. There is no way to display user-defined character on Windows 95 with Internet Explorer.

For Netscape 4 for Windows and HotJava for Windows, you must change the browsers' font-properties file to register a class for character-set conversion. For details, refer to the files in the `\ondemand\hod\samples\fonts\dbc_s_udc` directory after installation. This contains a sample class for character-set conversion, a sample font-properties file, and instructions.

Font-size does not change on OS/2 - fix

If a session is configured for host code page 930 or 939 and you are using Netscape 2.02 for OS/2, the font size does not change when you change the size of the session window.

The problem is fixed by APAR IC21598.

Euro dollar symbol copy and paste

When you copy the Euro dollar symbol to the clipboard, it may display incorrectly because the proper fonts are not installed. You must install new operating system fonts to display new symbols, such as the Euro dollar.

Print Screen when the marked area trim-rectangle contains split DBCS characters

When the marked area trim-rectangle contains split DBCS characters, Print Screen prints only the parts of DBCS characters that are contained inside the marked area trim rectangle.

Some half-width characters cannot be displayed in a TSO environment

In a TSO environment, some half-width characters from the 1364, 1371, 1309 and 1399 code pages cannot be displayed. This is a TSO problem that awaits a fix of the TSO codepages.

Korean DBCS with Netscape 4.7.2 on AIX

Due to a platform limitation, you cannot input Korean DBCS on a Host On-Demand client running Netscape 4.7.2 on AIX.

Print Screen on Windows 2000 in a session using monospaced fonts

If your monospaced Host On-Demand session font, such as MS Gothic or MS Mincho, is mapped to one of PAGES' fonts, you must set your Windows 2000 printer driver to Don't Substitute fonts in order to Print Screen. MS Gothic and MS Mincho fonts are mapped to PAGES' Gothic and PAGES' Mincho fonts by default, which results in incorrect print screen output.

Corrupted National language characters in text entry fields

If the National Language characters you are typing into a text entry field are corrupted when using a Host On-Demand client with a Netscape browser, copy the font.properties.xx file from the *hostondemand/hod/samples/fonts/win32/* directory to the *netscape/communicator/program/java/classes* directory (where xx is the two letter language code for your language).

Selection box appears to truncate top lines on AIX with Netscape DBCS

If you are using Host On-Demand on AIX with Netscape and you attempt to select several lines of Double Byte Character Set (DBCS) text, your browser will move the top edge of the selection box down half a line so that it runs through the middle of the line of characters. If you then attempt to cut this selected text, all of the text will disappear except the half of the line of characters that was above the top edge of the selection box. In other words, it will appear that you have not cut all of the text that you wanted to.

However, this is not so. If you refresh the screen, the line of half-characters will disappear, and if you paste the text that you previously cut, all of the text that you had originally selected, including the truncated text, will appear.

This is a limitation of Netscape.

DBCS filenames and paths are not displayed for Netscape on AIX

Filenames and paths that contain Double Byte Character Set (DBCS) characters cannot be displayed properly when using Netscape on AIX. This problem appears mostly in functions that use the File Browse feature such as the File Transfer GUI and the Import/Export facility. This is a limitation in the File Browse feature in the browser on the AIX platform.

Some DBCS characters appear with '{?}' on T,P,J,K-OS/2 4.0 Merlin

When a Host On-Demand client runs on Netscape 4.61 for the OS/2 platform, the following Double Byte Character Set (DBCS) PC codes are displayed with {?} :

Traditional Chinese:

a148, a153, a1b8, a1f3, a1b9, a1e3, c6e6

Simplified Chinese:

a1a4, a1ee, a1ef, a3bf

Japanese:

815c, 8160, 81f1, 8199, 817c, 81f2, 81f3

Korean:

a1a4, a1a9, a1d9, a1da, a2bb, a2a6, a2c1, a2d0, a2da, a2bd, a2d1, a2db, a2cd, a3bf, a2bf, a2ce, a2dd, a2bb, a2cf

This is a problem with Netscape running on the OS/2 platform.

DBCS input field's character can't output to other fields on Netscape for AIX

When Host On-Demand clients are running on Netscape for AIX, the Double Byte Character Set (DBCS) input field's characters can't output to other fields after users type characters in DBCS input field and then hit the Enter key. This is a constraint of Netscape running on AIX.

DBCS Gaiji mapping table

Host On-Demand users can remap UDC (user-defined characters) between the host and the client's personal computer (PC). The Host On-Demand server provides a UDC mapping editor. Users can use this editor to change the mapping of user defined-characters between the host and the PC. Before users start a session (3270, 5250, 3270 host print), they can edit the configuration property of this session in order to use customized UDC mapping instead default mapping.

DBCS GB18030 support

Host On-Demand supports GB18030-2000 code page (GB18030 phase 1 only / CCSID 1388) character display and 3270/5250 unicode/PC code (GB18030) file transfer. The 3270 host print is also supported, but 5250 host print depends on OS/400 supported.

Scroll bar does not work normally on Netscape 4.61 with JDK1.1.8 for OS/2 platform

If you click any one of the session icons on the first row on the Configured Session window and then attempt to scroll down, the display will not stop at the bottom. Instead the display will cycle back to the first row. However, if you click icons on the other rows, scrolling will behave normally.

This is a limitation of Netscape 4.61 with JDK1.1.8 for OS/2 platform.

Last interim Hangeul is not displayed

Because of the way the JVM composes Korean characters and the timing involved, typing "rkrk" sends only one Korean character to Host On-Demand to be displayed instead of two.

This is a limitation of the JVM.

Korean "Won" and Japanese "Yen" appear as backslashes (\) on Korean and Japanese Win32 browsers

Because of a JVM problem, the following double-byte characters appear as backslashes (\):

- Won (Korean)
- Yen (Japanese)

This is a browser limitation on Korean and Japanese Win32 platforms.

The IME toolbar mistakenly turns on when clicking sessions using Java 2

On Traditional/Simplified Chinese Windows, the IME toolbar might launch and turn to On when you single click icons on the Host On-Demand desktop. However, when you launch Host On-Demand terminal windows, IME will be turned to Off and you can input SBCS characters correctly.

On-the-spot conversion

On DBCS Linux/AIX, the candidate window might be located just below the Host On-Demand session window instead of below the current cursor location. This is because Linux/AIX IM (Input Method) does not have the interface to locate the candidate window to the desired position. The actual location is determined by Linux/AIX IM.

Auto IME function does not work on any DBCS version of Linux

The Auto IME function does not work on any DBCS version of Linux because Linux IM (Input Method) does not have such an interface. As before, users need to turn IME on manually when DBCS is inputted.

Auto IME with Simplified and Traditional Chinese

On Simplified and Traditional Chinese Windows, the Auto IME function does not work if the default SBCS (English) IME is set as the current IME. To use Auto IME, manually set DBCS IME as the default IME using Control Panel > Keyboard > Input Locales.

IME toolbar disappears on Simplified Chinese OS/2 Warp 4 with IBM Java2 Plugin

On Simplified Chinese OS/2 Warp 4 with IBM Java2 Plugin, the IME toolbar disappears when DBCS is inputted. This problem is caused by OS/2 and will be fixed with the next FixPak release of Simplified Chinese OS/2 Convenience Pak2. However, DBCS can be still be input.

Auto IME on Korean Windows

The Auto IME function on Korean Windows works with IBM Java2 1.3.1 SR2 or later.

Understanding bidirectional language support (Arabic and Hebrew)

- [Understanding bidirectional Arabic support](#)
- [Understanding bidirectional Hebrew support](#)
- [Understanding bidirectional editing functions](#)
- [Understanding bidirectional support for Database On-Demand](#)
- [Remapping bidirectional keys](#)
- [Setting the ScrRev key function](#)
- [Summarizing shortcut keys](#)
- [Configuring a CICS Gateway session](#)
- [Macro Support With BIDI Sessions](#)
- [Bidirectional support for FTP client in UTF-8 mode](#)
- [Bidirectional support for Copy As Table](#)
- [Printing Right-to-left file](#)
- [Understanding the limitations of bidirectional support](#)

- Help for [VT bidirectional language support \(Arabic and Hebrew\)](#) is available.
- To use bidirectional support with the Screen Customizer/LE interface, you need an Arabic operating system to support an Arabic graphical user interface session or a Hebrew operating system to support a Hebrew graphical user interface session.



Understanding bidirectional Arabic support

- [Understanding bidirectional Arabic limitations](#)
- [Using installation tips](#)
- [Configuring a workstation](#)
- [Transferring files](#)
- [Understanding bidirectional keyboard functions for 3270](#)
- [Setting the Arabic character shape selection functions](#)
- [Configuring Host On-Demand for iSeries](#)
- [Understanding Operator Information Area \(OIA\) indicators](#)
- [Allocate space for LamAlef](#)
- [Printing in Arabic language](#)

Understanding bidirectional Arabic limitations

The bidirectional Text Assist Function is not supported for Host On-Demand for iSeries. Therefore, you cannot run bidirectional OfficeVision/400.

Using installation tips

If the active font control file does not include the Arabic character set, copy one of the properties files listed below to replace font.properties.ar. The font.properties.ar file is located in one of the following directories:

- `..\netscape\communicator\program\java\classes` for Netscape 4.x
- `..\Program Files\JavaSoft\JRE\1.3.0_01\lib` for Netscape 6.0

The new properties files are located in the `hostondemand\hod\samples\fonts\bidi` directory. Right-click one of the links

below to download the appropriate file.

- [font.properties.win](#) for Windows (using Netscape 4.x)
- [font.properties.ar.13](#) for Windows (using Netscape 6.0)
- [font.properties.aix](#) for AIX
- [f_ar.prp](#) for OS/2

Configuring a workstation

For a Host On-Demand server installation, first you must customize an Arabic HTML file using the Deployment Wizard. To customize a HTML file for Arabic, set the appropriate code page.

Setting the code page

To set the appropriate code page:

1. Click Preload Options on the Additional Options window in the Deployment Wizard.
2. Select Codepages2 in the preload tree.
3. Select Arabic.


Configuring an Arabic session

To configure a workstation for Arabic, set the appropriate code page and enable numeric or symmetric swapping.

Setting the code page

To set the appropriate code page:

1. Right-click a 3270 or 5250 configured session icon.
2. Click Properties.
3. Select 420 Arabic Speaking for the Host Code Page.
4. Click the Screen tab and either select the bitmap font ARB3270 to be the active font for display or leave the default font, Courier, which is the system font.

 For Host On-Demand for Windows 95 you can also select ARB3270 for printers with drivers that allow bitmap fonts.

Setting the swapping option

To set numeric or symmetric swapping for Arabic:

1. Click View.
2. Add a checkmark next to the Numeric Swapping or Symmetric Swapping option.

Changes are immediately reflected in the active session.



Numeric swapping is a 3270-only feature and is not available for an iSeries session.

Transferring files

For Arabic, when transferring files between the PC and the host, the available PC code pages are:

- 864: Arabic PC code pages for OS/2
- 1256: Arabic PC code page for WIN95/NT
- ISO 8859-6 (01089) (ar_A): Arabic ISO code page for AIX
- 1046: Arabic code page for AIX
- Unicode (UTF-8): PC File is in UTF-8 encoding
- Unicode (UCS2): PC File Data is in Unicode range

Unicode Transfer options (UTF-8 and UCS2) are not available in the PC code page list. To enable Unicode Transfer options, complete the following:

In the Receive Text File or Send Text File Options on the OS/400 tab in the File Transfer Defaults window, replace the keyword ASCII with either Unicode (UTF8) or Unicode (UCS2), depending on the user requirement.

Unicode transfer options are available only in 5250 sessions.

To set the Bidi properties:

1. Click Actions > File Transfer Defaults.
2. Select the appropriate PC code page.
3. Select the Bidi settings:
 - For right-to-left host file orientation, check the Right-To-Left Host File Orientation checkbox.
 - For left-to-right host file orientation, check the Left-To-Right Host File Orientation checkbox.
 - For right-to-left PC file orientation, check the Right-To-Left PC File Orientation checkbox.
 - For left-to-right PC file orientation, check the Left-To-Right PC File Orientation checkbox.
 - For visual PC file type, check the Visual PC File Type checkbox.

Visual PC File Type is only highlighted for PC code page 864, AIX-1046, and Unicode. Select a PC code page first, then select the PC file type.

If you select Visual PC File Type during Unicode Transfer, Arabic data is received in the shaped FE range. Otherwise Arabic data is received in the 06 isolated range.

- For Lam-Alef Expansion, check the On checkbox.
- For Lam-Alef Compression, check the On checkbox.
Lam-Alef options are valid for only PC Codepage 1256, AIX-1089, and Unicode with PC file Type not Visual.
- For Symmetric Swapping Option Enabled, check the On checkbox.
- For Round Trip Option Enabled, check the On checkbox.
The Round Trip option disables the reversal of numerals if preceded by Arabic characters.
- Select the appropriate Numerals Shape: nominal, national, or contextual.

4. Click OK. Changes are saved for each session.

If you don't set Bidi settings, the following defaults are used:

- PC Default CodePage 1256
- Implicit PC File Type
- Left-To-Right PC File orientation
- Left-To-Right Host File orientation
- Lam-Alef Expansion On
- Lam-Alef Compression On

- Symmetric Swapping On
- Round Trip On
- Nominal Numerals Shape

Understanding bidirectional keyboard functions for 3270

This section describes the keys and functions that are unique to bidirectional 3270 for Arabic. These key combinations are identical to previous versions of 3270.

The keys unique to bidirectional 3270 are:

Language selection

The key combination Ctrl+N or Ctrl+L allows you to change the language layer. If the language layer is Latin, pressing Ctrl+N changes the language layer to Arabic. If the language layer is Arabic, pressing Ctrl+L changes the language layer to Latin.

Screen reverse

The key combination Ctrl+S reverses the screen image. If the screen orientation is left-to-right, pressing Ctrl+S reverses the screen image right-to-left. If the screen orientation is right-to-left, pressing Ctrl+S reverses the screen image to left-to-right.



Screen reverse does not reverse the operator information area.

When the screen orientation is changed, the language layer changes to the default language of the new screen orientation. If the screen is reversed to right-to-left, the language changes to Arabic. If the screen is reversed to left-to-right, then the language changes to Latin.

If the swapping of symmetric characters is enabled, the inversion of the screen causes directional characters to be replaced by their counterparts.

If the swapping of numeric characters is enabled, the inversion of the screen causes Hindi numerals to be replaced by their Arabic counterparts and the Arabic numerals to be replaced by their Hindi counterparts.

Field reverse

The key combination Ctrl+F toggles the field orientation to either opposite to or the same as the screen orientation. In most cases, the field direction is the same as the general screen direction. However, sometimes it is necessary to have a field whose direction is the opposite of the screen direction. The Field Reverse function allows such transitions. When this function is activated, the typing direction reverses, but the existing text in the field and the screen image do not change. When activated, this function creates a temporary change which stays in effect as long as the cursor remains within the field, or until Field Reverse is activated again.

If the function is activated while the cursor is at the beginning of a line or field, the cursor jumps to the end of the line or field, so that the reversed field begins logically from that position. Otherwise, the cursor remains in its position and allows natural and correct editing of existing texts whose direction is the opposite of the screen direction.

Auto field reverse

The key combination Ctrl+R toggles the auto field reverse mode for the current screen orientation.

Auto field reverse affects the automatic selection of the field orientation of unprotected fields:

- When auto field reverse is enabled, upon initial entry to an alphanumeric field, the field orientation will be set to right-to-left (for both left-to-right and right-to-left screen orientations).
- When auto field reverse is enabled, upon initial entry to a numeric field, the field orientation will be set to left-to-right (for both left-to-right and right-to-left screen orientations).
- When auto field reverse is disabled, upon initial entry to a field (whether numeric or alphanumeric), the field orientation is always set equal to the screen orientation.

Push and end push

This function is activated by the key combination Ctrl+P and allows the entering and editing of text whose direction is opposite from the field direction. When this function is activated, the cursor orientation is reversed, the language layer is changed accordingly, and a push segment is created.

End push, activated by the Ctrl+O (the letter "O") key sequence, ends the push mode.



In Windows mode, push is also activated by the Shift+NumLock key sequence and end push is also activated by the Shift+NumPad/ key sequence.

When you end the push mode, the cursor jumps to the end of the push segment, and its direction changes to the original direction. You can also perform end push by pressing any field exit keys (for example, Cursor Up or Cursor Down) or an aid key (for example, Enter).

The push function has two secondary modes:

Boundary mode

This mode is activated upon entering push mode. In this mode, the cursor remains in its position, and the typing of additional characters pushes the text in the direction opposite from the field direction. To indicate this boundary mode, the cursor has a block shape.

Edit mode

This mode is activated when the cursor is moved from its boundary position into the push segment area. In this mode, you can edit the text within the push segment, while typing in the field's natural direction.

AutoPush

This function is activated by the key combination Ctrl+A and helps the terminal operator type mixed left-to-right and right-to-left text. When enabled, reversed segments are automatically started and ended, according to the entered character or the selected language layer. This mode relieves the operator from manually pressing Push, as it is automatically invoked.

- In right-to-left fields, typing a digit or a Latin letter causes the automatic initiation of push, without language change. Further Latin letters or digits will continue the push mode; any other character automatically terminates push mode. This feature allows you to type Arabic text with embedded numbers or Latin words without using push or end push.
- In left-to-right fields, typing an Arabic character or special character causes the automatic initiation of push, without language change. Typing any digit or Latin character causes the automatic termination of the mode. This allows you to type Latin text with embedded Arabic words using language layer selection rather than push and end push.



Setting the Arabic character shape selection functions

There are five shape selection keys: one for Contextual Shape Determination (CSD) and four for Specific Shaping modes (Base/Isolated, Initial, Middle, Final). The default Shaping Mode is CSD.

The keys unique to bidirectional 3270 are:

Contextual Shape Determination (CSD) key

Pressing this key sets the shaping mode to Contextual Shape Determination (CSD), which is the default. Note that contextual shape determination is performed only for right-to-left text entered or modified by the operator. This key toggles between CSD and Base mode.

Pressing any of the Specific shape selection keys disables CSD.

The character Alef-Madda in the operator information area indicates that CSD is selected. This function is initiated by the key combination Ctrl+D.

Specific Shape Selection keys:

- Base/Isolated: Initiated by the key combination Ctrl+I





- Initial: Initiated by the key combination Ctrl+T
- Final: Initiated by the key combination Ctrl+E
- Middle: Initiated by the key combination Ctrl+M

Pressing one of the above keys disables CSD and sets shaping mode to the selected value. Arabic letters subsequently typed will have the selected shape.

Some Arabic characters do not have middle, initial, or final shapes. In this case, if you enter one of those characters where the requested shape does not exist, the closest shape is selected according to the following rules:

- Instead of initial, isolated is selected.
- Instead of final, isolated is selected.
- Instead of middle, final (if it exists) or isolated is selected.

The selected Shaping Mode is shown in the operator information area:

- Isolated GHEIN  indicates Base/Isolated Shaping Mode
- Initial GHEIN  indicates Initial Shaping Mode
- Middle GHEIN  indicates Middle Shaping Mode
- Final GHEIN  indicates Final Shaping Mode

Field shape key

Pressing the key combination Ctrl= causes the shaping of the Arabic data present in the current field or line. The cursor position remains unchanged.

Field de-shape key

The key combination Ctrl- de-shapes the Arabic data present in the current field or line. All Arabic letters are converted to their Base/Isolated shapes.

Configuring Host On-Demand for iSeries

The keys and functions unique to bidirectional Host On-Demand for iSeries are:

Language selection

This function is activated by the key combination Ctrl+N or Ctrl+L and allows the changing of the language layer. If the language layer is Latin, pressing the Ctrl+N key combination changes the language layer to Arabic. If the language layer is Arabic, pressing the Ctrl+L key combination changes the language layer to Latin.

Screen reverse

This function is activated by the key combination Ctrl+S and reverses the screen image. If the screen orientation is left-to-right, pressing this key combination changes the screen image to right-to-left. If the screen orientation is right-to-left, pressing this key combination reverses the screen image to left-to-right.

Note that the operator information area is not reversed by this operation.

When the screen orientation is changed, the language layer changes to the default language of the new screen

orientation. If the screen is reversed to right-to-left, the language changes to Arabic. If the screen is reversed to left-to-right, the language changes to Latin.

The inversion of the screen causes directional characters to be replaced by their counterparts.

Field reverse

This function is activated by the key combination Ctrl+F and toggles the field orientation to either left-to-right or right-to-left. The text in the field is not inverted. The cursor orientation is set equal to the new field orientation and the language layer is selected accordingly.

If the cursor is in the first logical position of a field or line and you select the field reverse function, the cursor skips to the other side of that field or line, which now becomes the first logical position. If the cursor is not in the first position of the field or line and you select the field reverse function, the cursor remains in its position and allows natural and correct editing of existing text.

Close

This function is activated by the key combination Ctrl+C and is provided so that the data entered in one keying direction can be concatenated with the data that was previously entered in the opposite direction. It operates as follows:



- All embedded nulls are removed from the current line.
- Concatenated text is moved to the right boundary of the field (if the field direction is right-to-left) or to the left boundary (if the field direction is left-to-right).
- The cursor direction is set to the field direction.
- The language layer is set to the default for the field direction.
- If the screen orientation is now left-to-right, the cursor is positioned at the first null to the right of the concatenated text.
- If the screen orientation is now right-to-left, the cursor is positioned at the first null to the left of the concatenated text.








Base

This function is activated by the key combination Ctrl+B and is a toggle that activates or deactivates the Automatic Shape determination function for Arabic right-to-left text. It is valid only when processing right-to-left Arabic text. If it is pressed in a left-to-right field, an operator error 0027 results.

Understanding Operator Information Area (OIA) indicators

In the host session, the bottom line of the screen is called the Operator Information Area (OIA). This line is always displayed from left-to-right. For the Arabic environment, the following symbols have been added:

- Language indicator:
 - Isolated EIN  Current language, Arabic
 - E: Current language, English
- Screen direction:
 - S> : Left-to-right screen direction
 - <S : Right-to-left screen direction
- Typing direction:
 - => : Left-to-right direction
 - <= : Right-to-left direction
 -  : Left-to-right push direction (3270 Only)

-  : Right-to-left push direction (3270 Only)
- Auto field reverse function active (3270 only):
 - 
- Auto field reverse for numbers (3270 only):
 - N
- Auto push active indicator (3270 only):
 - P
- Arabic character shape mode:
 - The character Alef-Madda  indicates CSD mode
 - Isolated GHEIN  indicates Base/Isolated Shaping Mode
 - Initial GHEIN  indicates Initial Shaping Mode (3270 Only)
 - Middle GHEIN  indicates Middle Shaping Mode (3270 Only)
 - Final GHEIN  indicates Final Shaping Mode (3270 Only)

Allocate space for LamAlef

5250 session

The Lam-Alef character is traditionally stored as a single character in files tagged with visual CCSID 420. To comply with the Implicit representation new CCSIDs introduced to the iSeries, the Bidi layout engine converts between Visual and implicit representation. This expands <Lam-Alef> ligature in visual representation to <lam> and <Alef> in implicit representation, consuming the spaces at the end of Arabic text, for example, the beginning of the English field.

When the <Lam-Alef> is converted to implicit format and the blank spaces at the beginning of the field are not sufficient to expand into <Lam> and <Alef> it is lost and replaced by the <SUB> control character.

Solution

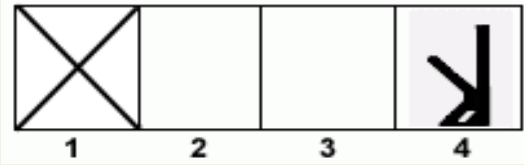
Leave a blank space at the beginning of the field for each typed Lam-Alef character and prevent users from entering data there, as the layout engine uses the blank space to expand the <Lam-Alef> character.

This new behavior is supported only by Host On-Demand emulation and not by the terminal.

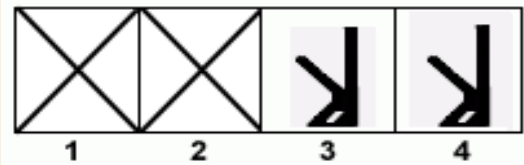
The following example illustrates the intended behavior.

Example

- Assume an input/output field length of four.
- Arabic text writing, typing, and reading starts from the right and progress towards the left. The user starts typing Lam-Alef in any arbitrary position. The emulator protects position one to allow the Bidi layout engine to use this space in the <Lam-Alef> expansion. The crossed locations (X) are protected so the user can not type in these locations.



- If the user types <Lam-Alef> in position four, then position three. The emulator protects position one and two to allow the Bidi layout engine to use this space in the Lam-Alef expansion.

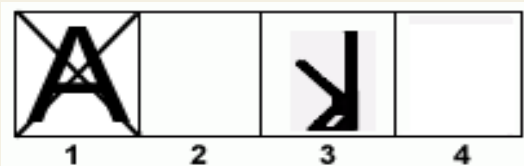


- If the user attempts to type an additional character, the Keyboard locks. The user must press the <RESET> key to continue. An error message that says Cursor in protected area of display appears.

The Allocate space for LamAlef option appears on the Language tab in the session configuration window. Users should enable this option.

Limitations

- If the leftmost character in the field is not blank before entering the Lam-Alef, the layout engine cannot properly expand it. Host On-Demand prevents the user from typing LamAlef and an error message appears that says Key not valid at this time. This limitation occurs with the paste and delete functions.



- In RTL Continued field, the allocate space for LamAlef allocates space from the start position of the first line of the field. If you fill the first line in the RTL Continued Field, you cannot type LamAlef anywhere in the remaining lines of the field.

Printing in Arabic language

5250 session

Using host printing transformation, install the 864 Arabic fonts on the printer or install the AFP fonts on the iSeries system.

3270 session

Using printer definition files (PDFs), do the following:

1. Install the 864 Arabic fonts on the printer.
2. In the PDF, define the escape sequences of the fonts that you want to use. You can get the font escape sequences by printing out the font names from the printer menus. For example:

 /* Naseem (1 0 V (s 0 p 1 5 h 9 v 0 s 0 b 3 T */

 NSM EQU 1B 28 31 30 56 1B 28 73 30 70 31 35 68 39 76 30 73 30 6233 54

3. Add the escape sequence of the font that you want to use to the START_JOB escape sequence in the PDF. For example: START_JOB=CUL CBP NSM /*
 Switch to Arabic Font */

4. Compile the PDF to get the printer definition table (PDT) file.

Related topics

- [Printing from a host to a workstation printer \(5250\)](#)
- [Printing from a host to a workstation printer \(3270\)](#)

Understanding bidirectional Hebrew support

The bidirectional Hebrew support in 3270 enables the program to emulate an English/Hebrew 3270 display terminal. Special language and bidirectional functions are added to the list of standard functions supported by the emulation program.

[Setting a font control file](#)

[Configuring a workstation](#)

[Transferring files](#)

[Understanding Hebrew and bidirectional functions](#)

[Summarizing bidirectional key combinations for 3270](#)

[Summarizing bidirectional key combinations for 5250 sessions](#)

[Understanding the Operator Information Area \(OIA\) in terminal emulation mode](#)

[Understanding the keyboard layout](#)

Setting a font control file

If the active font control file does not include the Hebrew character set, or if you have any problems with Hebrew characters appearing, copy the properties file listed below to replace font.properties.iw. The font.properties.iw file is located in one of the following directories:

- ..\netscape\communicator\program\java\classes for Netscape 4.x
- ..\Program Files\JavaSoft\JRE\1.3.0_01\lib for Netscape 6.0

The new properties file is located in the hostondemand\hod\samples\fonts\bidi directory. Right-click the link [font.properties.iw.win](#) to download the file for Windows.

Configuring a workstation

For a Host On-Demand server installation, first you must customize a Hebrew HTML file using the Deployment Wizard. To customize the HTML file for Hebrew, set the appropriate code page.

Setting the code page

1. Click Preload Options on the Additional Options window of the Deployment Wizard.
2. Select Codepages2 in the Preload tree.
3. Click Hebrew.

Configuring a Hebrew session

To configure a workstation for Hebrew, set the appropriate code page and font.

1. Right-click a 3270 or 5250 configured session icon.

2. Click Properties.
3. Select 424 Hebrew (New Code) or 803 Hebrew (Old Code) for the Host Code Page.
4. Click the Screen tab and either select the bitmap font HEB3270 to be the active font for display or leave the default font, Courier, which is the system font.

Transferring files

For Hebrew, when transferring files between the PC and the host, the available PC code pages are:

- 862: Hebrew PC code pages for OS/2
- 1255: Hebrew PC code page for WIN95/NT
- ISO 8859-8: Hebrew ISO code page for AIX
- 856: Hebrew code page for AIX
- Unicode (UTF-8): UTF-8 encoding
- Unicode (UCS2): PC File Data is in Unicode range

Unicode Transfer options (UTF-8 and UCS2) are not available in the PC code page list. To enable Unicode Transfer options, complete the following:

In the Receive Text File or Send Text File Options on the OS/400 tab in the File Transfer Defaults window, replace the keyword ASCII with either Unicode (UTF8) or Unicode (UCS2), depending on the user requirement.

Unicode Transfer options are available only in 5250 sessions.

To set the Bidi properties:

1. Click Actions > File Transfer Defaults.
2. Select the appropriate PC code page.
3. Select the Bidi settings:
 - For right-to-left host file orientation, check the Right-To-Left Host File Orientation checkbox.
 - For left-to-right host file orientation, check the Left-To-Right Host File Orientation checkbox.
 - For right-to-left PC file orientation, check the Right-To-Left PC File Orientation checkbox.
 - For left-to-right PC file orientation, check the Left-To-Right PC File Orientation checkbox.
 - For visual PC file type, check the Visual PC File Type checkbox.
Visual PC File Type is only highlighted for PC code page 862, AIX 856, and Unicode. Select the PC code page first, then select the PC file type.
 - For Symmetric Swapping Option Enabled, check the On checkbox.
4. Click OK. Changes are saved for each session.

If you don't set Bidi settings, the following defaults are used:

- PC Default CodePage is 1255
- Implicit PC File Type
- Left-To-Right PC File orientation
- Left-To-Right Host File orientation
- Symmetric Swapping On

Understanding Hebrew and bidirectional functions

3270 can run as a native Windows application. The layout and user-interface functions in the Windows-based product conform to the IBM user-interface standard (SAA/CUA); they are similar to the layout and functions implemented in other IBM products, such as OS/2.

The functions and key sequences for Hebrew are:

Language selection

The key combination Ctrl+N or Ctrl+L allows you to change the language layer. If the language layer is Latin, pressing Ctrl+N changes the language layer to Hebrew. If the language layer is Hebrew, pressing Ctrl+L changes the language layer to Latin.

Screen reverse

The key combination Ctrl+S reverses the screen image. If the screen direction is left-to-right, the screen image is inverted and displayed from right-to-left. Pressing this hot-key again returns the screen to its original direction, left-to-right. When the screen orientation is changed, the language layer changes to the default language of the new screen orientation. If the screen is changed to right-to-left, the language changes to Hebrew. If the screen is changed to left-to-right, the language changes to Latin.



Screen reverse does not reverse the operator information area.

Field reverse

The key combination Ctrl+F toggles the field orientation to either opposite to or the same as the screen orientation. In most cases, the field direction is the same as the general screen direction. However, sometimes it is necessary to have a field whose direction is the opposite of the screen direction. The Field Reverse function allows such transitions. When this function is activated, the typing direction reverses, but the existing text in the field and the screen image do not change. When activated, this function creates a temporary change which stays in effect as long as the cursor remains within the field, or until Field Reverse is activated again.

If the function is activated while the cursor is at the beginning of a line or field, the cursor jumps to the end of the line or field, so that the reversed field begins logically from that position. Otherwise, the cursor remains in its position and allows natural and correct editing of existing texts whose direction is the opposite of the screen direction.

Auto field reverse

The key combination Ctrl+R sets the field orientation for you when you are entering data for mixed applications (Hebrew and English). This is done by automatically activating the Field Reverse function. The Auto Field Reverse mode is activated by the Ctrl+R key sequence, and can be applied independently for each screen orientation, left-to-right or right-to-left.

- If the auto field reverse option is activated on a right-to-left screen, the field reverse function automatically activates every time the cursor moves to a numeric field. The cursor then jumps to the leftmost position of the numeric field, to allow left-to-right typing of numbers.
- If the auto field reverse option is activated on a left-to-right screen, the Field Reverse function automatically activates only when the cursor moves to an alphanumeric field. The cursor then jumps to the rightmost position of the field, to allow right-to-left typing of Hebrew.

Initially, the auto field reverse option functions when the screen direction is right-to-left, and does not function when the screen direction is left-to-right. To terminate the auto field reverse mode, press Ctrl+R again.

Push and end push

The key combination Shift+NumLock enables you to type or edit text whose direction is the opposite of the field direction. When this function is activated the cursor orientation reverses, the language layer changes accordingly, and a push segment is created.

End push, activated by the Shift+NumPad/ key sequence, terminates the temporary mode. The cursor jumps to the end of the push segment, and its direction reverts to that of the field.

The push function has two secondary modes:

Boundary mode

This mode activates upon entering the push mode. In this mode, the cursor remains in its position, and the typing of additional characters pushes the text in the direction opposite to the field direction. To indicate this boundary mode, the cursor shape changes.

Edit mode

This mode activates when the cursor is moved from its boundary position into the push segment area. In this mode, you can change the text within the push segment, while typing in the text's natural direction.

Autopush

The key combination Ctrl+A makes work easier and more efficient when typing mixed text - Hebrew and English. When this mode is enabled, reverse segments initiate and terminate automatically, according to the entered character or the selected language layer. It relieves the operator from manually selecting push and end push. Autopush is especially useful for typing digits in Hebrew fields (right-to-left fields). The Autopush mode is activated by the Ctrl+A key sequence; it can be applied independently to fields whose direction is left-to-right or right-to-left. In this mode, the push and end push functions automatically activate according to the language of the text being typed. There is no need to worry about starting and stopping the push mode manually.

- In right-to-left fields, typing a digit or a Latin letter causes the automatic initiation of push, without language change. Further Latin letters or digits will continue the push mode; any other character automatically terminates push mode. This feature allows you to type Hebrew text with imbedded numbers or Latin words without using push and end push.
- In left-to-right fields, typing a Hebrew character causes the automatic initiation of push. Typing any digit or Latin character causes the automatic termination of the mode. This allows you to type Latin text with embedded Hebrew words by using language layer selection rather than push and end push.

Summarizing bidirectional key combinations for 3270

Function	Combination
Hebrew language	Ctrl+N
English language	Ctrl+L
Screen reverse	Ctrl+S
Field reverse	Ctrl+F
Auto field reverse	Ctrl+R
Push	Shift+NumLock
End push	Shift+NumPad/
Autopush	Ctrl+A

Summarizing bidirectional key combinations for 5250 sessions

Function	Combination
Hebrew language	Ctrl+N
English language	Ctrl+L
Reverse	Ctrl+R
Close	Ctrl+C
Screen reverse	Ctrl+S

Hebrew language

Same meaning as in 3270

English language

Same meaning as in 3270

Reverse

Pressing this key allows the operator to reverse the current cursor direction. It functions as follows:

- The cursor is repositioned according to the current cursor direction. When right-to-left, the cursor is placed

at the current left boundary location. When left-to-right, the cursor is placed at the current right boundary location.

- The cursor direction is then reversed; the Keyboard Layer you get depends on the new cursor direction.
- Insert mode is reset.

Close

By pressing this key, data entered in one key direction is joined with data that was previously entered in the opposite direction:




- All embedded null characters are removed from the current line (or field, if the field is contained on one line).
- Joined text is moved to the right boundary of the field if the field direction is right-to-left, or to the left boundary if the field direction is left-to-right.
- The remainder of the line (or the field, if contained on one line) is padded with null characters.
- The cursor direction is set to the field direction.
- If the cursor direction is now left-to-right, the cursor is positioned at the first null character to the right of the joined text. If the cursor direction is now right-to-left, the cursor is positioned at the first null character to the left of the joined text.
- Insert mode is reset.

Screen reverse

Same meaning as in 3270

Understanding the Operator Information Area (OIA) in terminal emulation mode

In the host session, the bottom line of the screen becomes an Operator Information Area (OIA). This line is always displayed from left to right. For the Hebrew environment, the following symbols have been added:

- Language indicator:
 - H : Current language is Hebrew
 - E : Current language is English
- Screen direction:
 - S> : Left-to-right screen direction
 - <S : Right-to-left screen direction
- Typing direction:
 - => : Left-to-right direction
 - <= : Right-to-left direction
 -  : Left-to-right push direction (3270 only)
 -  : Right-to-Left push direction (3270 only)
- Auto field reverse function active - bidirectional arrow:
 - 
- Auto field reverse for numbers:
 - N

- Autopush active indicator:
 - P

Understanding the keyboard layout

Two Hebrew keyboard templates (Bulletin and Old Code) are supplied with the product. The Old-Code template is similar to the Bulletin template, with the following exceptions:

- Shift+6 (s-6) produces the Greek Delta symbol (ASCII 235, hex EB), representing the old Israeli Lira, instead of the regular Cent symbol.
- Shift+7 (s-7) does not produce anything (the Ampersand symbol is not available in Old Code).
- In English language mode, unshifted English letters produce uppercase letters (A-Z), rather than lower case letters (a-z), whether Caps Lock is Yes or No.

Understanding bidirectional editing functions


To use the bidirectional cut, copy, and paste functions:

1. Right-click a configured session icon.
2. Click Properties.
3. Select the bidirectional Host Code Page.
4. Click Language.
5. Select the appropriate values for:
 - Numeral Shape
 - Text Type
 - Text Orientation
 - Round Trip
6. Click OK.

To change the cut, copy, and paste settings in an active Host On-Demand session:

1. Click Edit > Text Type > Text Orientation, Numeral Shape, or Round Trip
2. Select the appropriate values for bidirectional cut, copy, and paste:
 - Text Type - Visual or Logical
 - Text Orientation - Left to Right or Right to Left
 - Numeral Shape - National, Nominal, or Contextual
 - Round Trip - On or Off

Note: Round Trip disables the reversal of numerals if preceded by Arabic characters.

 The Numeral Shape menu option is available for Arabic sessions only.

Understanding bidirectional support for Database On-Demand

Bidirectional conversion and layout is provided so the user can send and retrieve bidirectional data correctly.

In Database On-Demand, the bidirectional support provides two functions:

File upload

This option enables the user to send bidirectional data to the iSeries. This data is converted from the PC code page to the iSeries code page, according to the PC file attributes, such as PC-File Type and PC-File Orientation as source attributes, and the field coded character set ID (CCSID) as target attribute. For example: CCSID 420 (Visual LTR), CCSID 62224 (Logical RTL)

The Database On-Demand detects the CCSID of the iSeries field automatically. However, the user needs to set the PC-File Type and PC-File Orientation attributes. Other PC file attributes default to:

- Numeral Shapes is Numerals_Nominal
- Text Shape is Text_Nominal
- Symmetric Swap is Swap_Yes

SQL wizard (to get the results of an SQL query as displayed records or as an output file)

This option enables the user to retrieve bidirectional data from the iSeries. This data is converted from the iSeries code page to the PC code page, according to the PC file attributes, such as PC-File Type and PC-File Orientation as target attributes, and the field coded character set ID (CCSID) as source attribute. For example: 420 (Visual LTR), 62224 (Logical RTL)

The Database On-Demand detects the CCSID of the iSeries field automatically. However, the user needs to set the PC-File Type and PC-File Orientation attributes. Other PC file attributes default to:

- Numeral Shapes is Numerals_Nominal
- Text Shape is Text_Nominal
- Symmetric Swap is Swap_Yes

A "BIDI options" tab appears on the Database On-Demand User Options panel if your system is configured for Arabic or Hebrew. This tab includes the following bidirectional options:

PC-File Type

This option specifies whether a transferred PC file is saved in logical or visual format. The default is Logical.

PC-File Orientation

This option specifies whether the transferred PC file is saved in left-to-right or right-to-left format. The default is Left-to-Right.

Remapping bidirectional keys

1. Right-click a configured session icon.
2. Click Properties.
3. Select the bidirectional Host Code Page.
4. Click Keyboard Remap.
5. Press the key you want to remap.
6. Select the bidirectional function that you want to remap.

The following bidirectional functions are available for 3270, 5250 and CICS bidirectional sessions:

- For 3270, 5250 and CICS:
 - Screen reverse
 - National keyboard layer
 - Latin keyboard layer
- For 3270 and CICS only:
 - Auto reverse
 - 3270 field reverse
 - Push

- End push
- Autopush
- Final
- CSD
- Initial
- Middle
- Isolated
- Field shape
- Field base
- For 5250 only:
 - Field reverse
 - Close
 - Base

Summarizing shortcut keys

To access functions that are often used, the following shortcut key combinations are available:

Function	Shortcut key
JumpNext	Ctrl+J
Print Screen	Ctrl+G
Exit	Ctrl+Q
Cut	Ctrl+X
Copy	Ctrl+Insert
Paste	Ctrl+V
Select All	Ctrl+K
Send File to Host...	Ctrl+Z
Receive File from Host...	Ctrl+Y
Play Macro	Ctrl+O (the letter "O")
Run Applet	Ctrl+1
Index	Ctrl+H

Setting the ScrRev key function

For 3270, 5250 and CICS bidi sessions, clicking ScrRev reverses the screen image.

Configuring a CICS Gateway session

1. Right-click a configured session icon.
2. Click Properties.
3. Select a bidirectional CICS Gateway Code Page:
 - 856 - Hebrew
 - 864 - Arabic
 - 916 - ISO Hebrew (8859_8)

- 1089 - ISO Arabic (8859_6)

4. Click OK.

Related tasks

- [Understanding VT bidirectional language support \(Arabic and Hebrew\)](#)

Macro Support with BIDI Sessions

When creating variables, updating variables, or extracting from Presentation space to variables, the variables are stored in Implicit format.

To correctly output BIDI data or variables to the Presentation Space using different MacroActions, complete one of the following:

1. Disable Translation of Host Action Keys with the MacroAction

In this case Transformation from Implicit Format to Visual Format (Presentation Space format) takes place, so the data will be displayed correctly on the Presentation Space.

2. Enable Translation of Host Action Keys with the MacroAction

The user must add appropriate BIDI Key Mnemonics within the Macro String, for example, Screen Reverse, Field Reverse, Push. In this case No Transformation from Implicit Format to Visual Format is done, as the data is sent by SendKeys() HACL method and data is processed Key-By-Key through Host On-Demand, that's why the user should insert the appropriate BIDI Key Mnemonics.

Bidirectional support for the FTP client in UTF-8 mode

File and directory names are passed to the FTP client as they are saved on the server. For example, files named on an AIX system using Logical VT terminal appear in incorrect order if the FTP client displays them in Visual mode. Therefore, when the FTP server is working in UTF-8 mode and the language is Arabic or Hebrew, the display mode should be Visual or Logical.

The Host On-Demand FTP client attempts to set the display mode according to client and server platform types, but sometimes the server platform information is not available. In those cases, you can manually set bidirectional reordering.

If you want the FTP client to perform bidirectional reordering, complete the following:

1. Right-click on the FTP session and select Properties.
2. On the More Advanced tab, select Yes for Force BIDI reordering.

Bidirectional support for Copy As Table

MS Excel Arabic and Hebrew Edition has an option named Default Orientation. If Default Orientation is right-to-left, the order of pasted columns is reversed relatively to how they are pasted with left-to-right Default Orientation. To make the Copy As Table operation compatible with MS Excel Arabic and Hebrew Edition, you can reverse the table columns.

To reverse the table columns, select Reverse Table Columns in the Edit window.

Printing Right-to-left files

This option is only for 3270 Printer sessions.

A file created by an application on a RTL screen is displayed with reversed lines on a LTR screen. If you attempt to print the file, the lines print in reverse. To print the file as it appears on the RTL screen, complete the following:

- On the Language tab in the 3270 Printer session properties, select Yes for Print RTL file. The default is No.

- In runtime, select File > Print RTL file.

Print RTL file is available only for printing to Windows printers or Adobe PDF files.

Understanding the limitations of bidirectional support

Netscape supported by Database On-Demand

Database On-Demand supports Netscape Version 6.0 only. There is no support for Netscape 4.7.

Arabic SHADA character displayed as a block

The Arabic character SHADA is displayed as a block when using the Screen Customizer/LE interface, because of a limitation in the Courier and Monospaced fonts regarding the display of Unicode Shaped characters.

Using the Arabic Tatweel character

The Arabic character Tatweel cannot be used with Java 1.4 unless the current system keyboard is set to Arabic.

Corrupted national language characters in text entry fields

- If the National Language characters you are typing into a text entry field are corrupted when using a Host On-Demand client with a Netscape browser, copy the font.properties.xx file from the hostondemand/hod/samples/fonts/win32/ directory to the netscape/communicator/program/java/classes directory (where xx is your two letter language code).
- When you use Database On-Demand, host characters 0x5f and 0x4A are not displayed correctly with Internet Explorer 5.5 on the Windows 2000 platform.

Using special fonts for 3270 native Windows printing

- For Arabic codepages, install the font Typing Arabic on your workstation. The font file, Typearb.ttf, is located in the lib\samples\fonts\win32 subdirectory.
- For Hebrew codepages running on Windows without Hebrew support, install the font Cumberland Hebrew on the client and server. The font file, Cumrheb.ttf, is located in the lib\samples\fonts\win32 subdirectory.

URL Hotspots on RTL screen

Since there is no way to know if a host application that works on a RTL screen displays URL names reversed or not reversed, URL names are recognized in both directions. For example, both www.ibm.com and moc.mbi.www are recognized as URL names on a RTL screen.

Understanding Hindi enablement

[Reviewing supported platforms](#)

[Specifying Hindi monospaced font for Windows 2000 and Windows XP](#)

[Configuring a workstation](#)

[Modifying a session configuration](#)

[Switching keyboards between Hindi and Latin](#)

[Identifying language shift status](#)

[Using cut, copy and paste functions](#)

[Using file transfer](#)

[Understanding Hindi clusters](#)

[Understanding the behavior of the arrow, Delete and Insert keys](#)

[Understanding the limitations of Hindi support](#)

Reviewing supported platforms

Hindi sessions run on the Windows 2000 and Windows XP operating systems. Select the Indic language group while installing Windows. After installation, you can change the language group to Indic:

1. Select Settings > Control Panel > Regional Options > General.
2. Select Indic for the Language settings for the system field.
3. Reboot the system.


Supported browsers

The following browsers are supported for Hindi enablement of Host On-Demand:

- Netscape 4.7
- Netscape 6.0
- Internet Explorer 5.0
- Internet Explorer 6.0

Supported plugins

The IBM Java 2 Plugin (JRE1.3) and Sun Java 2 Plugin (JRE1.4) are supported for Hindi enablement of Host On-Demand.

 Sun Java 2 Plugin (JRE1.3) is not currently supported because the plugin is not composing Hindi Unicode characters.

To use the IBM Java 2 Plugin (JRE1.3) with supported versions of Netscape and Internet Explorer, do the following:

1. Download the IBM Java 2 Plugin from <http://www.ibm.com/developerworks/java/>
2. Uninstall the Sun Java 2 Plugin, if it is installed.
3. Install the IBM Java 2 Plugin.
4. In the directory where you installed the IBM Plugin, change the IBM security provider referenced in the `\jre\lib\security\java.security` file from **security.provider.2=com.ibm.crypto.provider.IBMJCA** to **security.provider.2=com.ibm.crypto.provider.IBMJCE**
5. Restart the browser.

To use the Sun Java 2 Plugin (JRE1.4) with supported versions of Netscape and Internet Explorer, do the following:

1. Download the Sun Java 2 Plugin (JRE1.4) from <http://java.sun.com>
2. Install the Sun Java 2 Plugin with JRE 1.4
3. Restart the browser.

Specifying Hindi monospaced font for Windows 2000 and Windows XP

Host On-Demand uses Monospaced Devanagari font for a Hindi session on Windows 2000 and XP. To install Monospaced Devanagari font on the client:

1. Download the font file to the client in the Windows font directory.
2. Change the browser settings as follows:
 - o For Internet Explorer, assign the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM\Font Alias\Courier the key value of Devanagari MT Narrow.

The key font alias may not exist in your system. Use the following steps to create a font alias:



1. Under the registry entry Java VM, create a KEY called Font Alias.
 2. For the KEY Font Alias, create a VALUE called Courier.
 3. For the VALUE Courier, update the data with the hindi font name Devanagari MT Narrow.
 4. Reboot your system.
- o For Netscape, replace the existing font.properties file with the supplied one. The file normally exists in the directory \Program files\Netscape\Communicator\Program\Java\Classes.
 - o For the IBM plugin, replace the existing font.properties file in the \Program files\ibm\java13\jre\lib directory with the supplied one.
 - o For the Sun plugin, replace the existing font.properties file in the \jdk1.4\jre\lib directory with the supplied one.

Configuring a workstation

To configure a workstation for Hindi, set the appropriate code page:

1. Click the Add sessions button at the bottom of the client window.
2. Right-click the 5250 display session to add.
3. Click Copy.
4. Enter the destination address and select 1137 Hindi for the Host Code Page.
5. Click OK.
6. Click Close to close the Add Sessions window. An icon is added to the Configured sessions window.

Modifying a session configuration

To modify a workstation configuration for Hindi:

1. Right-click a configured 5250 display session icon.
2. Click Properties.
3. Change the required information on each tab.
4. Click OK.

Switching keyboards between Hindi and Latin

To switch the keyboard between Hindi and Latin, use the following key combinations:

Default key mapping	Language
Ctrl+N	Hindi
Ctrl+L	Latin

Identifying language shift status

If the keyboard is in Hindi language shift, the indicator HI appears on the Operator Information Area (OIA).

Using cut, copy and paste functions

Cut, copy and paste are supported on Hindi display mode. You can copy and cut text using the keyboard. When using keyboard functions (Shift+arrow key) for marking text, the trimming rectangle appears at the Hindi cursor position.

Using file transfer

For Hindi, when you transfer files between the PC and the host, select 1137 Hindi for the Host Code Page.

Because Hindi language is supported only in UNICODE, the ASCII transfer option does not apply to Hindi file transfer. Use the UNICODE transfer option to transfer a file in TEXT mode. When the session has the Hindi code page, the transfer option UNICODE is the default for TEXT mode transfer.

Transfer PC files in UNICODE format. If you do not use UNICODE format to transfer a PC file, the following error message can appear:

ECL0146 Error while reading from the local file system.

Understanding Hindi clusters

A cluster is a single character on the screen that internally might be represented by more than one character. Two or more individual characters in Hindi can combine to form or compose a glyph or cluster. The number of characters in a cluster varies.

In order to find the number of characters in a cluster, Unicode Ligation and ISCII rules will be used. The 15 Unicode Ligation rules defined by the Unicode Consortium can be found in the book *The Unicode Standard Version 3.0* by the Unicode Consortium, published by Addison Wesley Publishing Company.

Other than the Unicode rules, Indian Script Code for Information Interchange (ISCII) rules also identify a cluster. The ISCII rules are as follows:

Rule 1: Letter I(\u0907) + Nukta(\u093C) forms Letter Vocalic L(\u090C)

Rule 2: Vowel Sign Vocalic R(\u0943) + Sign Nukta(\u093c) forms Vowel Sign Vocalic Rr(\u0944)

Rule 3: Candrabindu(\u0901) + Sign Nukta(\u093c) forms Om(\u0950)

Rule 4: Letter Vocalic R(\u090b) + Sign Nukta(\u093c) forms Letter Vocalic Rr(\u0960)

Rule 5: Letter Ii(\u0908) + Sign Nukta(\u093c) forms Letter Vocalic LI(\u0961)

Rule 6: Vowel Sign I(\u093f) + Sign Nukta(\u093c) forms Vowel Sign VocalicL(\u0962)

Rule 7: Vowel Sign Ii(\u0940) + Sign Nukta(\u093c) forms Vowel Sign Vocalic LI(\u0963)

Rule 8: Danda(\u0964) + Sign Nukta(\u093c) forms Sign Avagraha(\u093d)

Rule 9: Consonant+Halant(\u094d)+Halant(\u094d)+Consonant forms Consonant + Halant(\u094d) + ZWNJ + Consonant

Rule 10: Consonant+Halant(\u094d)+Nukta(\u093c)+Consonant forms Consonant + Halant(\u094d) + ZWJ + Consonant

Also based on the ISCII rules, the Host On-Demand Hindi enablement allows a maximum of five consonants to form a cluster. If a cluster contains more than five consonants, only the first five consonants are treated as a cluster. The remaining characters form a separate cluster based on the five-consonant rule.

Understanding the behavior of the arrow, Backspace, Delete, and Insert keys

The arrow, Backspace, Delete, and Insert keys have some special behaviors in Hindi sessions because of the formation of clusters.

Some of the terms used to describe these behaviors include:

Character or Code Point

The smallest component of written language that has semantic value

Glyph or Cluster

The shape that characters can have when they are displayed

A single glyph or cluster can correspond to a single character or to a number of characters. To understand clusters and their formation, refer to [Understanding Hindi clusters](#).

Arrows

To move the cursor from one glyph or cluster to another on the screen using the left and right arrow keys, position the cursor at the beginning or end of a cluster, depending on the key pressed. These positions are known as boundary positions. Cluster support is available for Hindi for the first time in Host On-Demand, Version 6.0.

Example

You type three characters: Devanagari letter KA, Devanagari sign Virama, and Devanagari letter SSHA. These three characters form a single glyph Devanagari letter K.SSHA. If the cursor is positioned after this glyph and you want to move the cursor to the character before the Devanagari letter K.SSHA, you need to press the left arrow only once.

Backspace

Place the cursor at the end of a cluster and press the Backspace key once to remove only a single Unicode character (a code point), not the entire cluster.

Example

You type three characters: Devanagari letter KA, Devanagari sign Virama, and Devanagari letter SSHA. These three characters form a single glyph Devanagari letter K.SSHA. Place the cursor at the end of the cluster and press the backspace key once to delete the Devanagari letter SSHA, not the entire cluster.

Delete

Place the cursor on a cluster and press the Delete key to delete the entire cluster instead of a single Unicode character (a code point).

Examples

Enter the Devanagari letter KA followed Devanagari vowel sign I. The glyph corresponding to Devanagari vowel sign I is displayed before the glyph corresponding to Devanagari Letter KA. When you press the Delete key, the Hindi cluster formed by the combination of Devanagari vowel sign I and Devanagari letter KA is deleted from the screen.

In another example, type three characters: Devanagari letter KA, Devanagari sign Virama, and Devanagari letter SSHA. These three characters form a single glyph Devanagari letter K.SSHA. Reach the glyph Devanagari letter K.SSHA by pressing the right arrow key and when the cursor reaches Devanagari letter K.SSHA, press the Delete key. The entire Devanagari cluster K.SSHA is deleted.

Insert

The Insert key enables inserting characters between clusters but not within clusters.

Example

YType three characters: Devanagari letter KA, Devanagari sign Virama, and Devanagari letter SSHA. These three characters form a single glyph Devanagari letter K.SSHA. You can either insert characters before the entire Devanagari cluster K.SSHA or after it, but you cannot insert characters within the cluster.

Understanding the limitations of Hindi support

- 3270, VT, and CICS emulation are not supported for Hindi sessions.
- 3270 printer sessions and 5250 printer sessions are not supported for Hindi.
- Hindi enablement is only supported on the Windows 2000 and Windows XP platform.
- Hindi enablement is not supported for Sun Java 2 Plugin (JRE1.3).

Thai language support

- [Understanding supported platforms](#)
- [Using Thai monospaced font](#)
- [Configuring Internet Explorer Thai](#)
- [Configuring Netscape Communicator](#)
- [Configuring a session to use Thai raster font \(THA3270\)](#)
- [Configuring a workstation with the Thai host code page](#)
- [Configuring your display mode](#)
- [Specifying Thai display composed mode](#)
- [Configuring a 3270 printer session \(PDT mode\)](#)
- [Creating a Thai PDT file for a Thai printer](#)
- [Configuring a 3270 printer session \(GDI mode\)](#)
- [Configuring a 3270 printer session \(Adobe PDF mode\)](#)
- [Configuring a 5250 printer session](#)
- [Configuring 3270 host graphics](#)
- [Configuring 5250 ENPTUI](#)
- [Using shortcut keys to switch keyboards between Thai and Latin](#)
- [Assign keys to Thai ancient characters](#)
- [Understanding Thai keyboard sequence checking](#)
- [Identifying the language shift indicator](#)
- [Using cut, copy and paste support](#)
- [Understanding the limitations of Thai support](#)

Understanding supported platforms

For Thai support, you must run the Host On-Demand client on one of the following Thai operating systems:

- Windows 95 Thai Edition
- Windows 98 Thai Edition
- Windows Millennium Edition (ME) Thai
- Windows NT 4.0 Thai with SP5 or later
- Windows 2000 Professional with Thai locales
- Windows XP (32-bit version) with Thai locales
- AIX 4.3.3, 4.3.4 Thai
- OS/2 Warp 4.0 Thai
- Linux RedHat 7.0, 7.1
- Thai Linux Extension (TLE) 4.1

The following browsers are supported for Thai enablement of Host On-Demand:

- Netscape Communicator 4.7 and 6.2
- Netscape Communicator 4.61 for OS/2 with JVM 1.1.8 or later. Download the latest version of Netscape Navigator for OS/2 and its JVM at [IBM OS/2 Software Choice](#).
- IBM Web Browser for OS/2 V1.2
- Microsoft Internet Explorer 5.0, 5.5 and 6.0
- Other browsers that support a Java 2 plug-in

Thai sessions can run on non-Thai operating systems (Windows, OS/2, Linux, and AIX) if you select [Thai raster font \(THA3270\)](#) for the font name. But, doing so has the following limitations:

- Unable to print Thai with print screen function.
- Unable to display Thai on the Abstract Window Toolkit (AWT) controls.

Using Thai monospaced font

Host On-Demand provides the Thai monospaced font Courier Thai for Windows Thai edition. To install the Courier Thai font file (courth.ttf):

1. [Download the file](#) to your client. Right-click the link to download the file.
2. Copy the file to the fonts folder located in the Windows control panel.

Configuring Internet Explorer

Microsoft Internet Explorer on Windows Thai Edition does not specify the correct font for Thai. To fix this:

1. [Download the registry file](#) to your client. Right-click the link to download the file.
2. Run regedit.exe (Registry Editor).
3. Click Registry > Import Registry File from menu. The Import Registry File dialog appears.
4. Select the registry file you downloaded in step 1, and click OK.
5. Close the Registry Editor.
6. Restart Internet Explorer with Host On-Demand.

Configuring Netscape Communicator

If the active font control file (font.properties) in Netscape Communicator does not include Thai character set, copy one of the properties files listed below to replace font.properties on Netscape 4.x or font.properties.th on Netscape 6.x.

The active font control file is located in the following directories:

- \Program Files\Netscape\Communicator\Program\Java\classes for Netscape 4.x
- \Program Files\JavaSoft\JRE\1.3.1_02\lib for Netscape 6.x

The new properties files are located in the *hostondemand\hod\samples\fonts\thai* directory, where *hostondemand* is your Host On-Demand installation directory. Right-click one of the links below to download the appropriate active font file and replace the active font control file with this new font.properties file.

- [font.properties.win](#) for Windows (using Netscape 4.x)
- [font.properties.th](#) for Windows (using Netscape 6.x)

For Netscape Communicator for OS/2 Warp 4.0 Thai, The active font control file (f_th.prp) already includes Thai character set.

Configuring a session to use Thai raster font (THA3270)

Thai raster font (THA3270) is similar to the sans-serif default font used by Personal Communications. To configure a session to use Thai raster font:

1. Right-click a configured session icon.
2. Click Properties.
3. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.
4. Click the Screen tab.

5. Select THA3270 for Font Name.

Configuring a workstation with the Thai host code page

1. Right-click a configured session icon.
2. Click Properties.
3. Select a Host Code-Page for Thai:
 - Select 838 Thai or 1160 Thai Euro for a 3270 or 5250 session.
 - Select Thai for a VT session.
 - Select 838 Thai or 1160 Thai Euro for a 3270 or 5250 print session.
 - Select 874 Thai for a CICS Gateway session.

Configuring your display mode

You can configure the Thai display mode from your session panel by doing the following:

1. Right-click a configured session icon.
2. Click Properties.
3. Select a Host Code-Page for Thai.
4. Click the Language tab.
5. Select Thai display mode from Thai Display Mode window.
6. Click OK.

You can also change the Thai display mode settings in an active Host On-Demand session:

1. On the View menu, click Thai Display Mode.
2. Select Thai display mode from Thai Display Mode window.
3. Click OK.

Specifying Thai display composed mode

You can specify the character composition and alignment for your text windows by indicating the display composed mode on the Thai Display Mode window. Specify one of the following modes:

Mode 1 - Non-compose mode

No character composition occurs in this mode.

Mode 2 - Composed mode

Thai characters are auto-composed in this mode. No column realignment is performed.

Mode 3 - Composed with space alignment

In this mode of composing, 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.

Mode 4 - Composed with EOF alignment

In this mode of composing, 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.

Mode 5 - Composed with space and EOF alignment (default)

This mode of composing performs the column realignment function of both mode 3 and mode 4. Mode 5 is the default Thai display mode.

Configuring a 3270 printer session (PDT mode)

To configure a 3270 printer session in PDT mode, do the following:

1. Right-click a 3270 Printer Session icon and select Properties.
2. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.
3. Click the Printer tab.
4. Set the User Windows Printer option to No.
5. Select the Printer Definition Table (PDT).
There are four [predefined Thai PDTs](#):
 - Thai ASCII text mode
 - Thai EPSON ESC/P Printer
 - Thai EPSON ESC/P2 Printer
 - Thai NEC Printer

If your printer is not included in the pre-defined Thai PDT list, [create a new PDT file or customize an existing PDT file for your Thai printer](#).

6. Click OK.



Thai support on 3270 Printer Session (PDT mode) is available on Thai dot-matrix printers only. The PCL printers and Postscript printers do not support Thai because Thai fonts are not available on these printers. Use [GDI mode](#) to print Thai on PCL printers and Postscript printers or use [Adobe PDF mode](#) to print Thai on Adobe PDF file..

Creating a Thai PDT file for a Thai printer

If none of the pre-defined PDTs are acceptable, you can create a new one. To create a PDT, first create a printer definition file (PDF) and then compile it to create a PDT.

To customize an existing PDF file for Thai:

1. Understand [a PDF's structure and the types of statements](#).
2. Add the THAI_CODE statement (THAI_CODE = YES) in the Session Parameter of the PDF file to indicate that this PDF/PDT file is for a Thai printer session only.
3. Remove all statements in Character Definition.
4. In Macro Definition, define a macro to a printer command that selects Thai printer font.
5. Add this macro to START_JOB in the Control Code section.
6. Save your new PDF file and copy it to the \pdfpdt\usrpdf directory.
7. Run the [PDT compiler](#) to create a user-defined PDT file.

Configuring a 3270 printer session (GDI mode)

To configure a 3270 printer session in GDI mode, do the following:

1. Right-click a 3270 Printer Session icon.
2. Click Properties.
3. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.
4. On the Printer tab, select Windows Printer in the Print to list.
5. Set the Use Printer Definition Table option to No.
6. Click the Page Setup tab.

7. Make sure the Font field says Courier Thai. If not, click Select Font and choose Courier Thai from the font list.
8. Click OK.

Configuring a 3270 printer session (Adobe PDF mode)

To configure a 3270 printer session in Adobe PDF mode, do the following:

1. Right-click a 3270 Printer Session icon.
2. Click Properties.
3. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.
4. On the Printer tab, select File in the Print to list.
5. Select Yes for Use Adobe PDF.
6. Type output directory in the File Path and Name field.
7. On the Page Setup tab, click Advanced Options.
8. Make sure CourierThai is selected in the Font list.
9. Click OK.


Configuring a 5250 printer session

To configure a 5250 printer session, do the following:

1. Right-click a 5250 Printer Session icon.
2. Click Properties.
3. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.

On the iSeries screen, do the following:

1. Specify that Host-Print Transform (HPT) will be used in the device description of a printer:
Host print transform TRANSFORM (*YES)
2. Specify your printer type and model in the parameter:
Manufacturer type and model . . MFRTYPMDL (*_____)
3. Make sure the character identifier parameter is capable of handling Thai language:
Character identifier: CHRID
Graphic character set 1176
Code page 838

 Thai support on 5250 Printer Session (HPT mode) is available on Thai dot-matrix printers only. The PCL printers and Postscript printers do not support Thai because Thai fonts are not available on these printers.

Configuring 3270 host graphics

To configure a 3270 host graphics session:

1. Right-click a 3270 configuration session icon.
2. Click Properties.
3. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.
4. Click Advanced tab.
5. Set Enable Host Graphics to Yes.

Configuring 5250 ENPTUI

To configure a 5250 ENPTUI session:

1. Right-click a 5250 configuration session icon.
2. Click Properties.
3. Select 838 Thai or 1160 Thai Euro for the Host Code-Page.
4. Click Advanced tab.
5. Set Enable ENPTUI to Yes.

Using shortcut keys to switch keyboards between Thai and Latin

To switch the keyboard between Thai and Latin, use the following shortcut keys:

Shortcut key	Function
Ctrl+N	Switch keyboard layout to Thai
Ctrl+L	Switch keyboard layout to Latin

Assign keys to Thai ancient characters

Some Thai ancient characters (Thai Angkhankhu, Thai Fongman, Thai Khomot, and Thai Yamakkan) are not included in the Thai keyboard layout.

To input these characters, you must assign a key to Thai ancient characters:

1. In a host session window, click Edit > Preference > Keyboard or click the Remap button on the toolbar.
2. Click the Key Assignment tab.
3. Select a Category.
4. Select the Thai ancient character you want to assign a key to.
5. Click Assign a Key.
6. Press the key you want to assign to the Thai ancient character.
7. After you have successfully assigned all the keys you want, click OK.

Understanding Thai keyboard sequence checking

Host On-Demand supports Thai Input Sequence check mode. This feature helps the user to eliminate all invalid sequence character-typing from the keyboard. When an invalid input sequence is entered, Host On-Demand makes a beep sound.

The rule of Thai keyboard sequence checking is taken from WTT 2.0 Thai standard defined by NECTEC (National Electronics and Computer Technology Center).

Identifying the language shift indicator

Host On-Demand Thai support indicates in the operator information area the language currently in use. If the keyboard is in Thai language mode, the indicator TH appears in the operator information area. No indicator appears if the keyboard is in the default Latin mode.

Using cut, copy and paste support

Cut, copy and paste are supported in all Thai display modes. You can copy and cut text using the keyboard. When using keyboard functions (Ctrl+arrow keys) for marking text, the trimming rectangle appears at the Thai cursor position.

Understanding the limitations of Thai support

Host On-Demand Download client with Java 2-enabled Web browsers

Java 2 has a stricter security model than the Java 1. You may encounter a Java security exception when running a Thai session on the Host On-Demand Download client with Java 2-enabled Web browsers. There are three possible solutions to this problem:

1. Use the Host On-Demand Download client with Problem Determination (HODDebug.html).
2. Use the Host On-Demand cached client for Java 2 browsers.
3. Use the [Deployment Wizard](#) to generate a set of Thai HTML files.

5250 ENPTUI function

There is no Thai support on word-wrap function or the Continued Entry field.

Database On-Demand

All Thai characters will be converted to question mark symbols (?) when exporting the database to a local file.

Thai Euro support

The Euro symbol only prints correctly if the font built into your printer supports the Euro symbol.

VT 100/220 enhancement

Double-width and double-height characters are not supported in a Thai session.

3270 GDI print mode

This mode is supported for Thai only on Win32 platforms.

Copy as Table

In Thai composed modes (mode 2-5), the Copy as Table function may produce incorrect output when you place Thai data into columns in other applications, such as a spreadsheet. You should use the Copy as Table function in the non-composed mode (mode 1) to get the correct output.

Understanding VT bidirectional language support (Arabic and Hebrew)

[Editing functions](#)

[Setting display options](#)

[Remapping bidirectional keys](#)

[Bidirectional support for printing in VT session](#)


[Understanding bidirectional Hebrew support](#)

[Understanding bidirectional Arabic support](#)

Editing functions

To change the cut, copy and paste settings in an active Host On-Demand session:

1. On the Edit menu, click Text Type, Text Orientation or Numeral Shape.
2. Select the appropriate values for bidirectional Cut/Copy & Paste:
 - Text Type - Visual or Logical
 - Text Orientation - Left to Right or Right to Left
 - Numeral Shape - National, Nominal or Contextual


 The Numeral Shape menu option is available for Arabic session only.

Setting display options

To set the bidirectional display options:

1. Right-click a configured session icon.
2. Click Properties.
3. Select a bidirectional Host Code Page.
4. Click Language.
5. Select the appropriate values for:
 - BIDI Mode - On or Off
 - Numeral Shape - National, Nominal or Contextual
 - Cursor direction - Left to Right or Right to Left
6. Click OK.

To change these settings in an active Host On-Demand session:

1. On the View menu, click Bidi Mode or Numeral Shape.
 2. Select the appropriate values:
 - Numeral Shape - National, Nominal or Contextual
 - BIDI Mode - On or Off
- 
 - The Numeral Shape and BIDI Mode menu options are available for Arabic session only.
 - The Cursor direction menu option is available for Hebrew session only in visual text mode.

Smart ordering on

A segment is a group of characters that have the same attributes. In this mode, text is ordered segment by segment. To enable this mode, select View > Bidi display options > Smart Ordering, and select On.

In this mode, you can indicate whether you want the underline attribute to be visible or invisible. Select View > Bidi display options > Show text attribute, and click on the On checkbox if you want the underlining to be visible.

Smart ordering off

In this mode, text is displayed with the default attributes. To enable this mode, select View > Bidi display options > Smart Ordering, and select Off.

Remapping bidirectional keys

1. Right-click a configured session icon.
2. Click Properties.
3. Select a bidirectional Host Code Page.
4. Click Keyboard Remap.
5. Press the key you want to remap.
6. Select the bidirectional function that you want to remap to that key.

The following bidirectional functions are available for a VT bidirectional session:

- Screen reverse (for logical text type only)
- National keyboard layer
- Latin keyboard layer
- Set/reset right-to-left cursor direction (for Hebrew session and visual text type only)
- Toggle between 7-bit and 8-bit character set modes (for Hebrew session only)
- Adjust the column heading (for Arabic session only)

Bidirectional support for printing in a VT session

To properly print Arabic or Hebrew text, the following should be implemented:

- Before submitting a printer job, send a start Esq-sequence to the printer that makes the printer use a national character set and an appropriate font
- Convert any national character from host codepage to printer codepage
- After completing a printer job, send a finish Esq-sequence to the printer that reinstates the printer's default settings

The start and finish Esq-sequences are printer-dependent. Currently, VT printing does not use Printer Definition Files (PDFs). But the PDF file is used for Bidirectional sessions to define host-to-printer ASCII translation and control codes sent at the start and the end of each host print job. See *Host Printing Reference* for more information about creating and using of Printer Definition Tables (PDTs) and Printer Definition Files (PDFs).

Choosing a printer definition file (PDF)

For a VT bidirectional session, select a PDF from the Printer tab of the Session Properties dialog box. For a non-VT bidirectional session, the Printer tab of the Session Properties dialog box includes a list of PDFs relevant for a VT session.

Creating a printer definition table (PDT) for a VT bidirectional session

To be used for a VT session, the PDT should include the parameter VT_PRINT?=x, where x is a number that identifies a language. The following identifiers are currently supported:

- 0 - Ignore
- 1 - Arabic
- 2 - Hebrew

If the parameter does not exist or is set to 0, the PDT should not be used for VT printing and is not displayed in the list of PDFs. If the parameter is set to one of currently supported languages, the PDF is not displayed in the Session Properties dialog box for a 3270 printer session.

Following is an example of a segment of a PDF file with parameters that are important for VT bidirectional printing. This PDF is designed for Hebrew printing on HP LaserJet 4 printer.

```
...
/* user-defined macros */
BEGIN_MACROS
...
...
SUL EQU 1B 26 64 33 44 /* Start Underline */
CUL EQU 1B 26 64 40 /* Cancel Underline */
SBP EQU 1B 28 73 31 42 /* Start Bold Printing */
CBP EQU 1B 28 73 30 42 /* Cancel Bold Printing */
CS1 EQU 1B 28 38 55 /* Roman 8 char set 1 */
```

```

CS2      EQU 1B 29 38 55          /* Roman 8 char set 2          */
SFT      EQU 1B 28 31 35 51 1B 28 73 30 70 31 30 2E 32 36 68 31 32 2E 30 76 30 73 30 62
39 38 54
ARA      EQU 1

/* Hebrew char set */

END_MACRO
/*****
/*          Control Codes          */
/*****
/* user defined sequences */
.....
START_JOB= CUL CBP SFT
END_JOB= CUL CBP CS1
VT_PRINT?=-ARA
.....
/*****
/*          Character Definitions          */
/*****
/*example: convert ASCII from 1255 (Hebrew codepage on Windows 98) to 862 (Hebrew
codepage used on printer)*/
/* the table is in format source=destination */
.....
E0=80
E1=81
E2=82
E3=83
E4=84
...

```

Other PDT parameters need not be processed for base bidirectional support and will be ignored for a VT session.

PASSTHRU mode support

The VT terminal uses PASSTHRU mode to send data to a printer without displaying it on a screen. The data can be plain text or binary data, such as image or Postscript text. See your VT terminal documentation for more information about PASSTHRU mode.

Some host applications send text that is already converted to the printer codepage. In these cases, the emulator should not perform any conversion.

By default, ASCII conversion for PASSTHRU mode is disabled, because the VT emulator cannot determine whether conversion is needed. To enable conversion, select Edit > Convert to printer codepage. For VT print modes other than PASSTHRU, ASCII conversion is enabled by default.

Understanding bidirectional Hebrew support

The bidirectional Hebrew support in VT enables the program to emulate an English/Hebrew VT 220 display terminal. Special Language and bidirectional functions are added to the list of standard functions supported by the emulation program.

[Configuring a workstation](#)

[Setting text types](#)

[Understanding Hebrew and bidirectional functions](#)

[Summarizing bidirectional key combinations for Hebrew](#)

[Understanding the Operator Information Area \(OIA\) in terminal emulation mode](#)

Configuring a workstation

1. Right-click a VT configured session icon.
2. Click Properties.
3. Select ISO Hebrew Supplemental (code page 916, 8-bit), or DEC Hebrew (code page 1349, 8-bit), or Hebrew NRCS (code page 1134, 7-bit) for the Host Code Page.
4. Click the Screen tab and either leave the default bitmap font HEB3270 to be the active font for display or select the system font, Courier.

Setting text types

The bidirectional session supports two text modes and their corresponding manipulation: Implicit (Logical) and Visual. In the Implicit text mode, characters are stored in same order that they are entered. The text is transformed into its visual form only when it is displayed. In the Visual text mode, characters are stored in the same way that they are displayed on the window. To switch between Visual and Logical text modes:

1. Right-click a configured session icon.
2. Click Properties.
3. Select a bidirectional Host Code Page.
4. Click Language.
5. Select the appropriate values for Text Type.
6. Click OK.



The visual text mode is available for Hebrew session only.

Understanding Hebrew and bidirectional functions

Language selection

The key combination Ctrl+N or Ctrl+L allows you to change the language layer. If the language layer is Latin, pressing Ctrl+N changes the language layer to Hebrew. If the language layer is Hebrew, pressing Ctrl+L changes the language layer to Latin.

Cursor direction

The key combination Ctrl+D allows you to change cursor direction. If current cursor direction is left-to-right, pressing Ctrl+D changes it to right-to-left, and back again. This function is allowed for visual text type only.

When cursor direction is set to right-to-left, this does not affect cursor addressing and moving, insert and delete characters, erase in line or erase in display. The following functions are affected by right-to-left cursor direction setting:

- o Backspace (the cursor moves one position to the right)
- o Carriage return (the cursor moves to the rightmost position on the current line)
- o Line feed (the cursor moves to the rightmost position of the next line)
- o Typing in the auto wrap mode (current line is continued from rightmost position of the next line).

Character set modes

This function is activated by the Ctrl+B key sequence and switches between 7-bit and 8-bit character sets. If the current character set is DEC Hebrew (8-bit) or ISO Hebrew Supplemental (8-bit), pressing Ctrl+B changes the current character set to Hebrew NRCS (7-bit). If the current character set is Hebrew NRCS (7-bit), pressing Ctrl+B loads one of two 8-bit character sets based on the following rule:

- o If the session is configured with one of the 8-bit character sets, that session's 8-bit character set will be loaded.
- o If the session is configured with 7-bit character set, ISO Hebrew Supplemental will be loaded.

The current language layer and cursor direction are not changed.

Screen reverse

This function is available for Logical text mode only. The key combination Ctrl+S reverses the screen image. If the screen orientation is left-to-right, press Ctrl+S to reverse the screen image to right-to-left. If the screen orientation is right-to-left, press Ctrl+S to reverse the screen image to left-to-right.

Summarizing bidirectional key combinations for Hebrew

Function	Combination
Hebrew language	Ctrl+N
English language	Ctrl+L
Toggle cursor direction	Ctrl+D
Toggle character set mode	Ctrl+B
Screen reverse	Ctrl+S

Understanding the Operator Information Area (OIA) in terminal emulation mode

In the host session, the bottom line of the screen is called the Operator Information Area (OIA). This line is always displayed from left to right. For the Hebrew environment, the following symbols have been added:

Language indicator	H - Current language is Hebrew E - Current language is English
Cursor direction	=> - Left-to-right direction <= - Right-to-left direction
Text type mode	I - Implicit mode V - Visual mode
Screen direction	S> - Left-to-right screen direction <S - Right-to-left screen direction

Understanding bidirectional Arabic support

The bidirectional Arabic support in VT enables the program to emulate an English/Arabic VT 220 display terminal. Special language and bidirectional functions are added to the list of standard functions supported by the emulation program.

[Configuring a workstation](#)

[Understanding Arabic language and bidirectional functions](#)

[Summarizing bidirectional key combinations for Arabic](#)

[Understanding the Operator Information Area \(OIA\) in terminal emulation mode](#)

Configuring a workstation

1. Right-click a VT configured session icon.
2. Click Properties.
3. Select ASMO-449 (7-bit) or ASMO-708 (8-bit) for the Host Code Page.
4. Click on the Screen tab and make sure that AVT3270 is the active font.

Understanding Arabic language and bidirectional functions

Language selection

The key combination Ctrl+N or Ctrl+L allows you to change the language layer. If the language layer is Latin, pressing Ctrl+N changes the language layer to Arabic. If the language layer is Arabic, pressing Ctrl+L changes the language layer to Latin.

Screen reverse

The key combination Ctrl+S reverses the screen image. If the screen orientation is left-to-right, pressing this key combination reverses the screen image to right-to-left. If the screen orientation is right-to-left, pressing this key combination reverses the screen image to left-to-right.

Column heading

Column heading mode causes blanks between columns of text to break insertions so the English titles to columns of data maintain their correct position. To enable the column heading mode, press the key combination Ctrl+K.

The following example illustrates the usefulness of the column heading.

When column heading is off:

Sent by host		Displayed by terminal (RTL screen)	
PCs	Printers	PCs	Printers
200	40	40	200
500	90	90	500

When column heading is on:

Sent by host		Displayed by terminal (RTL screen)	
PCs	Printers	Printers	PCs
200	40	40	200
500	90	90	500

Summarizing bidirectional key combinations for Arabic

Function	Key combination
Arabic language	Ctrl+N
English language	Ctrl+L
Screen reverse	Ctrl+S
Column heading	Ctrl+K

Understanding the Operator Information Area (OIA) in terminal emulation mode

In the host session, the bottom line of the screen becomes an Operator Information Area (OIA). This line is always displayed from left to right. For the Arabic environment, the following symbols have been added:

Language indicator	(AIN) Arabic character - Current language is Arabic. E - Current language is English
Screen direction	S> - Left-to-right screen direction <S - Right-to-left screen direction
Column heading	CH : CH - Column heading is set On.

Related tasks

- [Understanding bidirectional language support for 3270 and 5250 sessions \(Arabic and Hebrew\)](#)

Accessibility

Based on Section 508 of the US Rehabilitation Act, Host On-Demand offers new accessibility features to help users who have physical disabilities, such as restricted mobility or limited vision, use host sessions successfully. Features include keyboard equivalents for all actions (mouseless operation), support for display system settings for size, font, and color for user interface controls, and descriptive text for selected graphics. Currently, not all features are available for all screens; for example, the Administration Utility and the InstallShield are not yet fully accessible. To enable accessibility, select Java 2 or Auto Detect as the Client Java Type in the Deployment Wizard on the Additional Options page.

Users who want to take advantage of accessibility features must have Java 2. If you attempt to use accessibility features, your browser will be checked to determine if a Java 2 plug-in is available:

- If you are using Internet Explorer on a Windows platform and a Java 2 plug-in is not found, a panel will be displayed asking if you wish to install the Java 2 plug-in that was installed on the Host On-Demand Web server.
- If you are using Netscape Navigator on a Windows platform or are running on any platform other than Windows, you will be directed to contact your administrator for instructions on installing the Java 2 plug-in. For information on installing Java 2 on non-Windows platforms, see the Sun Microsystems Web site at <http://www.javasoft.com>.

Host On-Demand provides a Certificate Management utility (IKeyMan) with a new command-line interface that meets accessibility requirements. However, graphical-user interface (GUI) accessibility for the Certificate Management utility is not available in this release. For more information about IKeyMan, see [Planning, Installing, and Configuring Host On-Demand](#).

Accessibility features include the following:


[Keyboard equivalents](#)

[Descriptive text](#)

[Support for system display settings](#)

Keyboard equivalents

On host session screens, you can use keys or key combinations to perform operations that can be performed using the mouse. The following table contains some common Windows keyboard equivalents supported by Host On-Demand. For a more comprehensive list of Host On-Demand keyboard equivalents, refer to [Default Keyboard Mapping](#).

 Because keys and key combinations can be remapped using the [Keyboard Remap](#) function, the following shortcuts might be different than what is listed here.

Function	Keyboard equivalent
JumpNext	Ctrl+J
Print Screen	Ctrl+P
Exit	Ctrl+Q
Cut	Ctrl+X
Copy	Ctrl+C
Paste	Ctrl+V
Select All	Ctrl+A
Send File to Host...	Ctrl+S
Receive File from Host...	Ctrl+R
Play Macro	Ctrl+M
Run Applet	Ctrl+U
Index	Ctrl+H

Operating systems include standard shortcut keys as aids to accessibility. This documentation does not address operating system-specific accessibility features. Consult your operating system's documentation for more information about these features.

Descriptive text

Graphics and images that communicate meaningful information, such as links, headers, and banners, are available in text form for users who have impaired vision. Users simply position their mouse cursors over these graphics and images to display the descriptive text. For example, in this online help file, the graphic of the question mark in the top right corner is coded with the descriptive text "InfoCenter."

Other graphics and images that simply enhance the interface do not provide text descriptions.



Netscape 6 does not display descriptive text when the mouse cursor is positioned over graphics. Use View > Page Info > Images to see descriptive (alternate) text.

Support for system display settings

Host On-Demand supports system display settings, including settings for high contrast, size, font, and color for all user interface controls. Colors are not used to convey meanings but instead to provide enhancements.

Currently, not all Host On-Demand components support system display settings; for example, the Deployment Wizard and the Administration Clients do not support them.

Related topics

- [Remapping the keyboard](#)
- [Default characters and functions](#)
- [Thai shortcut keys](#)
- [BIDI shortcut keys](#)

Customize Toolbar



You can customize the toolbar buttons used for Host On-Demand sessions. After customizing the toolbar, settings are saved for future sessions.

Administrators can make their own customizations to toolbar buttons. On the Sessions panel of the [Deployment Wizard](#), select the session you want to customize and click Start. After the session starts, use the following instructions to customize the toolbar. Administrators can also [disable toolbar customization](#) so that it is not available to users.



Buttons on the Macro Manager toolbar cannot be customized.

Add Button

To add a new button, right-click on the toolbar and choose Add Button from the popup menu. In the Add Button panel, you can create a new button to launch an applet, play a macro, go to a specified URL, run an application, assign a keyboard function, or access basic menu items. After selecting a button, specify the text label you want to appear on the button in the Toolbar Text field. Provide a description of the button function in the Description field. This description will appear at the bottom of the Client window when the mouse rolls over a button. Click Add at the bottom of the selected tab and the new button will appear to the left of where you right-clicked. You can also add a button by selecting Edit > Preferences > Toolbar > Add Button. This will always add the button to the end of the toolbar.

Applet

Specify the full class name of an applet you want to launch.

Application

According to your platform syntax, specify the full application path followed by any application parameters. You can also use the Browse button to locate the path.

URL

Specify a URL address to open in your default browser.

Macro

Choose from the list of your pre-recorded macros. The original macro name will appear under Toolbar Text by default but can be changed. If the macro associated with a button is deleted, an error message will appear when the button is clicked.

Keystroke

Assign a keyboard function (from the Characters, Host Functions, or Custom Functions categories) to a toolbar button.

Certain keyboard functions are predefined with Host On-Demand for remapping. The [Custom Function Editor](#) allows you to define and maintain new keyboard functions, called custom functions, without having to edit HTML and Java script files. These new functions may be assigned to a toolbar button.

On the Keystroke page, choose from a list of keystrokes to create a button. Then, when you select that button, it will function as if the assigned keys have been pressed.

This option does not appear on FTP sessions.

Other Buttons

To add buttons associated with basic menu options click the desired button. The Toolbar Text and Description fields have default labels that can be changed.

Edit Button

To edit a button, right-click on the button icon and choose Edit Button from the popup menu. An edit panel appears allowing you to change the Toolbar Text and Description assigned to the button.

Choosing Custom Images

You can also choose your own images for custom buttons. A field lists the current icon used for the button you are creating or editing. Selecting the Change button (located next to the icon image) brings up the Change dialog, which allows you to type in the URL path for the icon image or to open a file dialog to select a .gif image to replace the current icon.

If the size of the .gif file is not 16x16, the file will be resized to 16x16; and the image may be unclear. Also, depending on size of the image file and download time, it may take awhile for the new image to appear.

Selecting the Default button resets the icon back to the default icon image.

Remove

To remove added buttons and spacers, right-click on the unwanted icon and choose Remove from the popup menu.

Insert Spacer

To create a space between buttons on the toolbar, right-click on a button and select Insert Spacer from the popup menu. The spacer appears to the left of the button where you right-clicked and the other buttons on the toolbar shift to the right.

Rearrange

To rearrange buttons on the toolbar, hold down either the right or left mouse button on a toolbar button, and then drag the button to the position that you want it to appear on the toolbar. If you drag a toolbar button off of the toolbar, it will not move and you will not lose the button.

Set to Default

You can revert to the toolbar as it appeared upon installation. Right-click on the toolbar and select Set to Default or select Edit > Preferences > Toolbar > Set to Default.

Related topics

- [Deployment Wizard](#)
- [Disabling functions](#)

Advanced tab



[Session Inactivity Timeout \(minutes\)](#)

[Reset Insert Mode on Aid key](#)

[Enable Host Graphics](#)

[Character Cell Size](#)

[Enable ENPTUI](#)

[Session ID](#)

[Start Automatically](#)

[Start in Separate Window](#)

[Auto-Connect](#)

[Auto-Reconnect](#)

[Auto-Start Applet/Macro Options](#)

[Auto-Start](#)

[Name](#)

[Parameter \(Optional\)](#)

[Scope](#)

[This Scope Only](#)

[Maximum Wait Time \(slp\)](#)

[Message Queue](#) (5250 printer session)

[Queue Library](#) (5250 printer session)

[Host Font](#) (5250 printer session)

[Use Customizing Object](#) (5250 printer session)

[Customizing Object](#) (5250 printer session)

[Object Library](#) (5250 printer session)

[Lock](#)

[Netname](#)

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.

Reset Insert Mode on Aid Key

If enabled 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 .

The default is No.

Enable Host Graphics

Enables the 3270 host graphics function. Host graphics is the display of lines, circles, ellipses, filled areas, images, and other graphics primitives as defined by the graphic orders of the IBM 3179G Color Graphics terminal. See the [supported orders](#) table for more information.

The default is No.

Character-Cell Size

The cell characteristics used for host graphics.

Select Automatic if you use host applications that redraw graphical pictures according to a Usable-Area Query Reply or a Character-Set Query Reply sent by the terminal. This is the case when you use host applications under GDDM, and in

some other graphical environments. Selecting Automatic causes the cell size returned by the Usable-Area Query Reply and the Character-Set Query Reply to change according to the Host On-Demand window size.

Select a fixed cell size if you use host applications that assume Terminal Usable Area to be a fixed coordinate space. Select the appropriate cell size for your application. For help selecting an appropriate cell size, refer to the [character-cell-size table](#).



Automatic is the recommended selection. Choose a fixed cell size only if the application does not display graphics correctly for the automatically-chosen size.

Click [here](#) more detailed information about character-cell size.

Enable ENPTUI

Enables Enhanced Non-Programmable Terminal User Interface (ENPTUI) support. ENPTUI enables an enhanced user interface on non-programmable terminals (NPT) and programmable work stations (PWS) over the 5250 full-screen menu-driven interface. This option is not available if the session is enabled for Screen Customizer.

In order to use data description specifications (DDS) grid functions such as GRDATR (Grid Line Attribute), GRDBOX (Grid Box), GRDLIN (Grid Line), and GRDRCD (Grid Record), the Enable ENPTUI option must be set to Yes. DDS grid line functions are supported only on DBCS.

Session ID

ID assigned to this session. Sessions are started in alphabetical order. The ID is displayed on the session window or tab. Automatic assigns and starts sessions in the order that they are created when Start Automatically is set to Yes.

Start Automatically

Session is started and connected (if Auto-Connect is Yes) when the client is loaded.

Start in Separate Window

If Yes is selected, 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-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.

Auto-Start Applet/Macro Options

Auto-Start

You can have an applet or a macro start at the same time as the session. Click the arrow and choose Applet or Macro, then type the name of an applet's class-file or the name of a macro in the box below. For an applet, only those applets that implement ECLAppletInterface or CustomInterface can run here.

Name

The applet's class-file name or the name of the macro that you want to auto-start.

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.

Host Code-Page (5250 printer session)

Specifies the table used to map EBCDIC codes from the host to appropriate ANSI graphics on the workstation. This option determines the list of available printers on the Printer tab. If you are using a DBCS language, you cannot select a host font. You must set it to the code page supported by the host system to which the session will connect.

The default is the code page that corresponds to the locale for which your workstation is configured.

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 only is 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.

Note: Directory Agent Discovery timeout and Service Agent Multicast timeout are both set with this value.

Message Queue

The name of the queue where operational messages for the printer device are sent.

If you specify the name of a display session here, messages relating to this printer device will be sent to that display session instead of to the default queue, QSYSQPR. A message queue exists for each display device and is assigned the same name as the device itself.

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, \$, @, #, . (period), and _ (underscore).

Queue Library

The name of the library where the printer message queue is located.

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, \$, @, #, . (period), and _ (underscore).

Host Font

The font used for a print file if a font is not specified by the application.

Use Customizing Object

Click Yes if you want to use an object file to format print data instead of using the formatting provided by the application.

Customizing Object

The name of a user-defined iSeries file that can be used to format the data for this device.

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, \$, @, #, . (period), and _ (underscore).

Object Library

The name of the iSeries system library that contains the customizing object file.

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, \$, @, #, . (period), and _ (underscore).

Lock

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

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.

Disabling Functions: Appearance



Items on the Appearance tab appear on the session window and can be accessed from the View menu. The state of these items is set in the session properties window. To prevent users from changing the state of items on this tab, lock them on the session properties window or disable Configure Sessions on the Desktop tab.

Functions

Select the Appearance functions for this user:

Toggle Toolbar State

Shows or hides the Toolbar in a display session window. The toolbar contains buttons to allow quick access to session functions. Toolbar appears in the View menu on the session window.

Toggle Toolbar Text State

Shows or hides the toolbar text on the buttons. Toggle Status Bar must be enabled for toolbar text to be displayed. Toolbar Text appears in the View menu on the session window.

Toggle Keypad State

Shows or hides the keypad in the display session window. The keypad displays the pf keys at the bottom of the session window. Keypad appears on the View menu and the toolbar of the session window.

Toggle Status Bar State

Shows or hides the status bar at the bottom of the session window. The Status Bar displays connection status messages and toolbar button descriptions. Status Bar appears on the View menu of the session window.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topic

- [Disabling functions](#)

Setting the display attributes




The Display attributes include cursor options and blinking text options. Click the button on the toolbar for "Set display cursor and text options".

Cursor options

Click the Allow blinking cursor checkbox if you want your host cursor to blink. Your cursor can blink as an underscore or a block. You can specify this in the [Screen tab of the Session Properties dialog box](#).

Blinking text options

1. Select how you want to display text with the blink attribute by doing one of the following:
 - Click the Blinking Text radio button if you want all fields with the blink attribute to blink.
 - Click the Host Color radio button if you want all the fields with the blink attribute to stop blinking and display the default host color for that field.
 - Follow these steps to map all the fields that have the blink attribute to a new color and disable blinking.
 1. Click the Mapped Color radio button.
 2. To select a new color, click the desired color in the color bar. To customize an exact color, click the Foreground Color or Background Color buttons to set RGB (red, green, and blue) values.
 If your text disappears, it could be mapped to the same color as your background. Select a different color.
2. Click the OK button to accept changes made and return to the session. Click the Cancel button to cancel all changes and return to the session. Click the Default button to overwrite the display attributes with the program default display attributes.

Related tasks

- [Screen tab in the Session Properties dialog box](#) describes how to change your cursor type.
- [Understanding session colors](#) gives more explanation about remapping colors in fields.



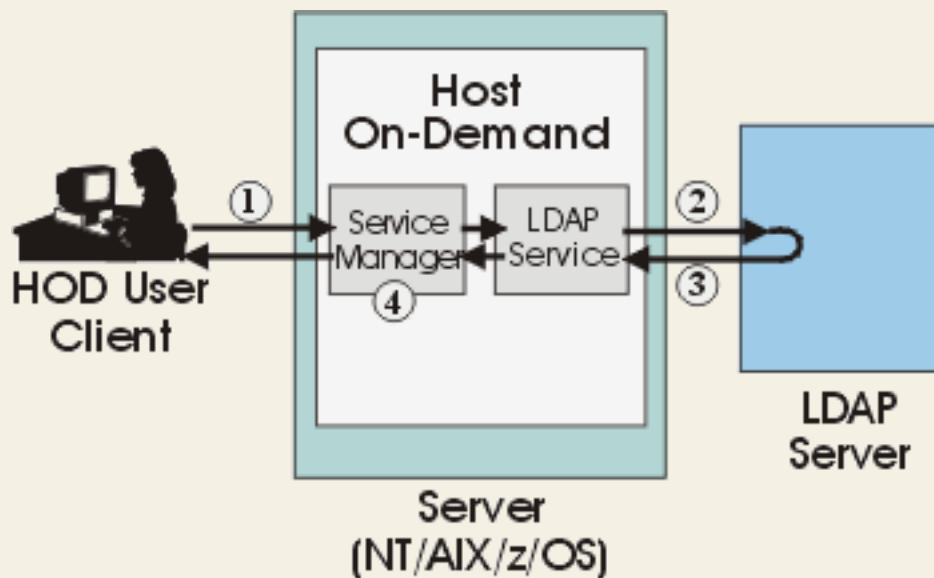
Native Authentication



The native platform authentication service allows users to logon to Host On-Demand using the same password as they would to logon 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:

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.



To allow users to have passwords with upper case letters, add `LowerCasePasswords = false` to the file `NSMPROP`, located in the `hostondemand\lib` directory. The service manager reads this file at startup and uses the `LowerCasePasswords` parameter to determine password case. Host On-Demand uses lower case letters by default.

Related Topics

1. [Native Authentication requirements](#)
2. [Installing the native platform authentication service](#)
3. [Starting the native platform authentication service](#)
4. [Configuring current users for native authentication](#)
5. [Enabling Windows NT users for native authentication](#)

Proxy Server tab



[Proxy Type](#)

[Proxy Properties](#)

[Proxy Server Name](#)

[Proxy Server Port](#)

[Socks Authentication Method](#)

[Socks Proxy Authentication Properties](#)

[Socks User ID](#)

[Socks Password](#)

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 servers 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 fields are 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 Socks v5 is selected as the Proxy Type.

Socks Authentication Method

Specify the authentication method that a Socks version 5 proxy server uses. Select one of the following:

Clear Text

The user ID and password for authenticating to the Socks proxy server are sent as clear text over the connection.

None

No authentication is used on the Socks proxy server.

Socks Proxy Authentication Properties

If you selected **Clear Text** as the **Socks Authentication Method**, enter the following properties:

Socks User ID

Enter the user ID for authenticating to the Socks version 5 proxy server.

Socks Password

Enter the password for authenticating to the Socks version 5 proxy server.



If the 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.

Related topics

- [Connecting to a host system through a proxy server](#)

Using Session 2 to configure and start a session



- Session1 and session2 do not support many new functions added to Host On-Demand V5 and later. In order to use these functions, use the [Deployment Wizard](#) instead.
 - A pre-configured session is not required. An HTML file created by these steps configures and launches a session.
1. Open session2.html with an ASCII text editor. Session2.html includes all the possible parameters and can be found in the **doc/samples/html** directory.
 2. Add or change [parameter](#) values as necessary.
 3. Save your changes and copy the file to the published directory on your Web server.
 4. Test the file to verify that it works correctly.

VT Display tab

[Terminal Type](#)

[Answer Back Message](#)

[New-Line Operation](#)

[Backspace](#)

[Local Echo](#)

[Cursor](#)

[Keypad](#)

[Autowrap](#)

[Reverse Screen Image](#)

[Move Cursor On Mouse Click](#)

[History Log](#)

[History Log Size](#)

[Lock](#)

Terminal Type (VT)

Defines the type of VT emulation you want to use, which depends on the types supported by your host system.

The default is VT420_7_BIT.

Refer to [VT 420 emulation limitations](#) for more information.

Answer Back Message

Use this field to enter the message to send to the host when the host inquiry command is sent to the terminal.

New-Line Operation (VT)

Specifies where the cursor will move when you press the New Line key.

- 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.

The default is CR.

Backspace (VT)

Defines the default behavior of the backspace key; however, the actual action of the key is determined by the host application.

- 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.

The default is Backspace.

Local Echo (VT)

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 then back to the display.

The default is No, which means that characters will display only once.

Cursor (VT)

- 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.

The default is Normal.

Keypad (VT)

- 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.

The default is Normal.

Autowrap (VT)

Click Yes if text must automatically continue to a new line when it reaches the margin on the current line.

The default is No.

Reverse Screen Image

Select this option to reverse the foreground and background colors.

Move Cursor On Mouse Click

Click Yes if you want the cursor to move when you click the mouse on the screen.

The default is Yes.

History Log

Click Yes if you want to be able to scroll through text that has moved off the screen.

The default is Yes.

History Log Size

Specifies the size of the buffer that the history log can use. Click the arrow next to the field to see the choices.

The default is 64k.

Lock

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Changing foreground or background colors

You can change foreground and background colors.

Click the basic or custom color of your choice.

To create a custom color, click Define custom colors, and use the scroll bars to set the new color. Color changes immediately display in the sample window.

To add a custom color, click Add to the custom colors, then click on any of five areas to save your new color.

Note:

If you try to add a new custom color without first clicking Add to custom colors, you will lose your new color. If this happens, click Reset Defaults to restore the default color settings.

Cached Client Client Help



The Cached Client download window appears:

- When the Cached Client is downloaded and installed for the first time.
- When the Cached Client is started and determines that components on the server are newer than components in cache. The newer components are downloaded to cache, replacing the older components.
- When components are needed for functions that are not initially downloaded by the Cached Client but are allowed by the administrator to be downloaded.

The Cached Client download window shows:

Status

Status of the files being downloaded, verified and installed.

Location

Location of the files being downloaded, verified and installed..

Current

Percent of the current file successfully downloaded, verified and installed..

Overall

Percent of all the files successfully downloaded, verified and installed..

Changing the Service Manager's configuration port

You can change the configuration port used by the Host On-Demand Service Manager and the clients. The default port of 8999 can be mapped to any available port number. If you are using Host On-Demand through a firewall, the port you set to be the configuration port must be opened on the firewall.

To change the configuration port to 12345, you need to make changes to the Service Manager, the clients and the configuration servlet (if you are using it):

To change the configuration port the Service Manager listens to:

1. Stop the Service Manager.
2. Go to the lib directory of the Host On-Demand server (for example, D:\hostondemand\lib).
3. Edit the NSMprop file to add

```
ConfigServerPort=12345
```

to the bottom of the file.

4. Restart the Service Manager.

There are other methods you can use to set ConfigServerPort for the Service Manager. Choose the easiest or most convenient method:

- Go to the lib directory of the Host On-Demand server (for example, D:\hostondemand\lib). Edit the NSMprop file to make the second parameter of CONFIGSERVER_PARMS "12345" instead of 8999 (this method provides compatibility with previous versions of Host On-Demand).
- Add /ConfigServerPort=12345 to the end of the command you use to start the Service Manager, or edit the script that is used to start the Service Manager so that the ConfigServerPort parameter is passed to it.
- On Windows NT, add the ConfigServerPort parameter to the registry entry for the Service Manager (on Windows NT the Service Manager runs as service):


```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IBMServiceManager\Parameters\AppParameters
```
- On OS/400, use CFGHODSM to add the ConfigServerPort parameter.

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:

1. First is a command line parameter, such as /ConfigServerPort=12345.
2. Second is the ConfigServerPort entry in the NSMprop file
3. Third is the setting of the second parameter of CONFIGSERVER_PARMS in the NSMprop file

Next, change the port the Host On-Demand clients use:

1. Go to the publish directory of the Host On-Demand server (for example, d:\hostondemand\HOD).
2. If necessary, create the file config.properties.
3. Edit config.properties to add

```
ConfigServerPort=12345
```

to the file.

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



If you need to edit config.properties for an z/OS server, first transfer the file in binary to an ASCII based system such as Windows or Unix. Edit the file and then transfer it back to the z/OS system in binary. If you need to create a config.properties file, do so on an ASCII system and 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, but files created or edited on z/OS are stored in EBCDIC.

When any parameter is set in a config.properties file, all clients will use that parameter. However, each client can be configured individually by adding parameters to the client HTML. You can use the Deployment Planning Wizard to build customized HTML client pages. The wizard sets applet parameters in the HTML it creates based on your input, so you don't have to learn the syntax and valid parameter values. It is recommended that you use the Deployment Planning Wizard to build client pages. The wizard can't be used to edit HTML pages you create manually. It also can't be used to edit HTML pages that are created with the wizard, but are later edited manually. If you find you need to manually modify the HTML, use the param tag inside the applet tag to set the ConfigServerPort. For example, you can add

```
<PARAM_NAME=ConfigServerPort VALUE=12345>.
```

to the applet tag in HTML file.

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:

1. First is the ConfigServerPort parameter set in the client HTML.
2. Second is the ConfigServerPort 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.

Related topics:

- [Using Host On-Demand with firewalls](#)
- [Configuring the configuration servlet](#)

Setting cached client parameters



You can selectively download Host On-Demand components to reduce the size of the cached client. By default, Host On-Demand base code is selected and cannot be deselected. The appropriate code-page group, based on a user's locale, is also selected. The administrator can customize the client HTML to define which components are available for initial download, which components the cached client can download as needed, and which components the cached client can't download. For example, if a component is upgraded on the Host On-Demand server, the cached client downloads the new component, and only the new component, the next time you start the cached client.

You can use the Deployment Wizard to build customized cached client pages. The wizard sets the applet parameters in the HTML it creates based on your input, so you don't have to learn the syntax and valid parameter values. We highly recommend that you use the Deployment Wizard to build client pages.

Applet parameters

The following parameters can be used to define and control cached client installations:

Parameter name	Description	Default value	Valid values
CachedAppletNonNetworkLoad	When set to true the cached client recognizes that it is being loaded from a lan drive or a CD, so it can present more helpful error messages and an end of installation message.	false	true, false
DebugCachedClient	Allows the cached client to output debug information.	false	true, false
DebugComponents	Determines if the cached client should load debug components instead of normal cached client components.	false	true, false
HODServer	Specifies a Cached client URL to a Host On-Demand v4 server so that you can manage Host On-Demand v4 Cached client upgrades gradually.	none	URL to a Host On-Demand v4 Cached client HTML page
InstallerFrameHeight	Allows for customization of Installer.html file so you can add installation specific HTML to the installation page.	250	integer
InstallerFrameWidth	Allows for customization of Installer.html file so you can add installation specific HTML to the installation page.	600	integer

PreloadCodeModules	The list of components to be downloaded initially. If there is no parameter specified, the default will be the Host On-Demand default cached client.	HABASE, HAPRINT, HA3270, HA3270B, HA3270T, HA3270P, HA5250, HA5250B, HA5250T, HA5250P, HA5250E, HACICS, HAVT, HAVTT, HAVTB, HATHAI, HADBCS, HABIDI, HAMACRT, HAMACUI, HAXFER, HA3270X, HA5250X, HASSL, HACHTAU, HASLP, HAHOSTG, HALUM, HACOLOR, HAKEYPD, HAKEYMP, HACP, HODBASE, HODIMP, HODTH, HODBI, HODSSL, HODAPPL, HODMAC, HODIMG, HAHINDI, HA5250H, HAFNTIB, HAFNTAP, HAFNTAR, HAFNTHE, HAFNTTH, HODHLL	list of components
UpgradePercent	Sets the percentage of users who can upgrade when a new version of Host On-Demand is available.	100	0 (no one is upgraded) - 100 (everyone is upgraded immediately)
UpgradePromptResponse	Allows the administrator to answer the upgrade prompt now, later, or background without displaying the prompt to the browser. When this parameter is set to prompt, the browser displays the choice.	prompt	now, later, background, prompt
UpgradeURL	Specifies a URL that is used to determine whether a user should be upgraded when a new version of Host On-Demand is available. If the retrieved document contains the word upgrade , the user is upgraded	<none>	URL, or file name relative to code base

Related topics

- [Cached Client \(HODCached.html\)](#)

Database On-Demand caption settings



Allows you to set the text attributes for the table caption text.

Caption Alignment

Specifies where you want the caption to appear in the HTML file relative to the table.

Caption Text Size

Specifies the text size of the caption.

Caption Text Style

Specifies the style of the caption. You can choose any number of style options.

OK

Applies the settings and exits the window.

Cancel

Exits the window without applying the settings.

Extracting a certificate



To extract a certificate:

1. Enter a URL or a path and file name or click Browse. Using a URL to send and receive files is dependent on the protocols your browser supports. Most browsers support http, https, ftp, and ftps.
2. Choose E-mail or Binary. E-mail saves the certificate to a file in armored-64 format. Binary saves it to a file in DER format.
3. Click OK.

Related topic:

- [Client authentication](#)

Server requesting certificate



The telnet server you are trying to connect to is requesting your certificate. Enter the location and password of your certificate. If you cannot make changes, the administrator that configured this session has locked these fields.

Requesting server

This is the name of the server to which you are trying to connect. Click Details to see more information about the server's certificate.

What do you want to do?

- Attempt to connect without my certificate
Whether you can connect without a certificate is dependent on the server you are trying to connect to. The server might give you access at a lower security level, or it might not allow any access without a certificate.
- Send my certificate
Click this if you have a certificate to send; then choose the Certificate Source:

If the certificate is stored on your system or in a file accessible using a URL:

1. Click PKSC12 or PFX file. Enter the URL or path and filename of the certificate that you want to send or click Browse to locate the file on the local file system. Sending and receiving files through URL's is dependent on the protocols your browser supports. Most browsers support http, https, ftp, and ftps.
2. Enter the password that was used to encrypt the certificate. If you don't know the password, ask your administrator or the person who requested and received your certificate.
3. Click View Certificate to see detailed information about the certificate you are sending. You must enter the location and password for the certificate before you can view it.

If your certificate is accessible through the Microsoft Internet Explorer Personal Certificate store, click Certificate in MSIE browser or security device, and select it from the Certificate Name drop-down box. Optionally, you can choose to send any certificate trusted by the server.

- Retrieve certificate before connecting can be selected, if you know that this host session will always require a certificate; this will streamline the handling for future sessions.
- How often to prompt
 - To be prompted each time the server requests a client certificate, click "Prompt on each connection".
 - To be prompted once each time HOD has been started, click "Prompt the first time after HOD is started".
 - 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.

Related topic:

- [Client authentication](#)

Viewing or saving a requesting server's certificate

To view detailed information about a server certificate, select a field from the Field list box. The value for the selected field is displayed in the Value field. The server certificate might not contain values for all the fields.

Click Extract to save the server's certificate. You can then [add it to the list of trusted CAs](#) (for locally- installed clients) or send it to your Host On-Demand administrator to add to the CustomizedCAs.class file on the server (for all other clients).

Click Show Issuer Certificate to view information about the issuer of the requesting server's certificate, if it's available. This provides an additional security check because you can check that the certificate is signed by whom you think.

Related topic:

- [Client authentication](#)

Viewing or saving issuer certificate information

Select a field from the Field list box. The value for the selected field is displayed in the Value field. The issuer's certificate might not contain values for all the fields.

Click Show Issuer Certificate to view certificate information about the issuer if it's available.

To save the certificate information, click Extract.

Related topic:

- [Client authentication](#)

Choose client certificate



If a client certificate has already been sent to the server, it will be displayed.

If the certificate is stored on your system or in a file accessible using a URL:

1. Click PKSC12 or PFX file. Enter the URL or path and filename of the certificate that you want to send or click Browse to locate the file on the local file system. Sending and receiving files through URL's is dependent on the protocols your browser supports. Most browsers support http, https, ftp, and ftps.
2. Enter the password that was used to encrypt the certificate. If you don't know the password, ask your administrator or the person who requested and received your certificate.
3. Click View Certificate to see detailed information about the certificate you are sending. You must enter the location and password for the certificate before you can view it.

If your certificate is accessible through the Microsoft Internet Explorer Personal Certificate store:

1. Click Certificate in MSIE browser or security device, and select it from the Certificate Name drop-down box. Optionally, you can choose to send any certificate trusted by the server.
2. Click View Certificate to see detailed information about the certificate.

Related topic:

- [Client authentication](#)

Selecting a character-cell size

Some host applications are sensitive to the cell size, especially those that were written without using GDDM. Use the following table to select an appropriate cell size based on the terminal for which the host application was written.

Select this size:	To match the cell size of:
9x12	3270 S3G 3179G/3192G (32x80)
9x16	3179G/3192G(24x80) 3472G (32x80)
9x21	3472G (24x80) Japanese 3270PC
13x22	newly created
13x29	Japanese 3270PC

Automatic is the recommended selection. Choose a fixed cell size only if the application does not display graphics correctly for the automatic cell size.

Related topics

- [Character cell size field](#)

Selecting a color scheme

To select a pre-defined set of remapped colors for your host session window:

1. Click Color on the toolbar.
2. Select a scheme from the Scheme selection list.
3. Click OK.

The host session screen changes to the foreground and background colors specified by the selected scheme. You can use the colors in the scheme or [change them](#).

Disabling Functions: Client Window



Items on the Client Window tab appear in the menu when a user right-clicks on a session icon in the Client window or the Add Sessions window.

Functions

Select the Client window functions for this user:

Add Sessions

Opens the Add Sessions window for selecting a session to add to the Client window. Add Sessions is a button that appears on the bottom of the Client window.

Delete Sessions

Deletes the selected configured session from the Client window or the Add Sessions window. Delete appears on the menu in both of those windows.

Change Session Properties

Configures the properties of a session. Properties appears on the menu in the Client window and the Add Sessions window.

Import Sessions

Imports an existing session from either Personal Communications V4.1 or later or a previously exported Host On-Demand session. Import is a button that appears on the bottom of the Add Sessions window.

Export Sessions

Exports a configured session to distribute to other users. Export Session appears on the menu in the Client window and the Add Sessions window.

Bookmark Sessions

Creates a bookmark in the browser for a session. Setup Bookmark appears on the menu of the Client window and the Add Sessions window.

Log Off

Logging off closes the Client window. Log Off is a button that appears at the bottom of the Client window. Closing the Client window ends all host sessions.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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.

Related topics

- [Client window](#)
- [Disabling functions](#)

Disabling Functions: Preferences



Functions

Select the preferences for this user:

URL Hotspots

Displays URLs as hotspots.

Confirm on Exit

Prompts you to confirm that you want to end your session.

Color Remap

Changes the colors for a display session. Color Remap appears on the Edit > Preference menu and on the toolbar of a session window.

Display Options

Allows fields to blink or not, and allows you to choose the color for blink fields of a display session. Display appears on the Edit > Preference menu and the toolbar of a session window.

Edit Keyboard Mappings

If enabled, allows users to assign, unassign, or reset key mappings and add or remove custom functions. If disabled, users will only be able to search for keys. Keyboard Mappings appears on the Edit > Preference menu and the toolbar of a display session window.

Lock Numeric Field

Allows you to type only the characters 0 through 9, -, +, period, and comma into fields defined by a host application as numeric. Numeric Field Lock is available for a 3270 or CICS display sessions only and appears on the Edit > Preference menu of a session window.

Toolbar Customization

Allows you to customize your toolbar.



Color Remap, Display Options, and Lock Numeric Fields do not apply to Screen Customizer sessions.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topic

- [Disabling functions](#)

Database On-Demand column heading settings

Allows you to set the text attributes for the table column headings.

Horizontal Alignment

Specifies the horizontal alignment for the table column headings.

Vertical Alignment

Specifies the vertical alignment for the table column headings.

Text Size

Specifies the text size for the table column headings.

Text Style

Specifies the text style for the table column headings. Any number of styles can be selected.

OK

Applies the settings and exit the window.

Cancel

Exits the window without applying the settings.

Selecting a session to configure



Select the type of session that you want to configure:

3270 Display

Access zSeries host applications.

5250 Display

Access iSeries server applications.

VT Display

Access UNIX server applications.

CICS Gateway

Access CICS applications (CICS gateway).

3270 Printer

Print from a 3270 session.

5250 Printer

Print from a 5250 session.

FTP

Access FTP servers.

Multiple Session

Define an icon that launches more than one session simultaneously, such as a 5250 display session and a 5250 printer session.

Import Session

Import a telnet session from Personal Communications or a previously-exported Host On-Demand session.

Configuring the configuration servlet



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, beginning with Host On-Demand version 6, you can avoid opening this port by customizing your clients to use the configuration servlet to access configuration information. "[Installing the configuration servlet](#)" in the Planning, Installing, and Configuring Host On-Demand guide contains instructions for installing the configuration servlet.

Configuration servlet parameters

The Host On-Demand configuration servlet recognizes these parameters. Check your Web server or servlet engine's documentation for instructions on how to pass parameters to a servlet.

Parameter	Default value	Description
ConfigServer	127.0.0.1	Host name or IP address of the Host On-Demand server.
ConfigServerPort	8999	Port number the Host On-Demand Service Manager listens to.
BufferSize	4096	Size of the buffer to use on buffered input or output streams.
PoolSize	5	Size of the buffer or socket pool to maintain. To turn off pooling, set PoolSize to 0.
Trace	false	When set to true, the configuration servlet writes servlet messages to the servlet engine log file, and to the browser when requested, for debugging purposes.
ShowStats	false	When set to true, allows the configuration servlet to return configuration information and statistics to browser requests.

Client parameters

The Host On-Demand clients, such as the Administration client (HODAdmin.html) and the Cached client (HODCached.html), recognize these parameters:

Parameter	Default value	Description
ConfigServer	Host On-Demand Server	Host name of the Host On-Demand server. The default value is taken from the hostname portion of the client's address.
ConfigServerPort	8999	Port number that the Host On-Demand Service Manager listens to.
ConfigServerURL	No default	Address or alias of the Host On-Demand configuration servlet.

You can set client parameters in the client's HTML code, in a *config.properties* file that you place in the publish directory (the same directory as the client HTML files on the server) or allow the clients to use default parameter values. When the clients load they first look for any parameters set in the HTML code. If none are present, they look for any parameters set in a *config.properties* file. If no parameters are set in *config.properties*, or if *config.properties* doesn't exist, the clients use default settings. The *config.properties* file can be an ASCII or a UTF-8 text file and contains *name=value* pairs. Lines that begin with the "#" are treated as comments.



If you need to edit *config.properties* for an z/OS server, first transfer the file in binary to an ASCII based system such as Windows or Unix. Edit the file and then transfer it back to the z/OS system in binary. If you need to create a *config.properties* file, do so on an ASCII system and 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*, but files created or edited on z/OS are stored in EBCDIC.

For example, to set the port number the client uses to contact the Service Manager from the default port 8999 to 12345, place *ConfigServerPort=12345* in the *config.properties* file on a line by itself.



When a *config.properties* file exists in the publish directory, all the clients use the same file. If you want some clients to use specific settings and others to use different settings, set the parameters in the client HTML pages.

There are two ways to specify the parameters directly in the client HTML. You can use the Deployment Planning Wizard to create a client with the parameters you specify, or you can modify the HTML manually. The wizard sets the applet parameters in the HTML it creates based on your input, so you don't have to remember the syntax and valid parameter values. It is recommended that you use the HTML Wizard to build HTML client pages. The wizard can't be used to edit HTML pages you create manually. It also can't be used to edit HTML pages that are created with the wizard, but are later edited manually. If you find you need to manually modify the HTML, use the param tag inside the applet tag to set the ConfigServerPort. For example, to set the port to 12345 set `<param name=ConfigServerPort value=12345>` in the applet tag in the HTML client.

Debugging information

You can access trace, configuration and statistical 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 `http://server_name/servlet_alias/HODConfig/trace` in your browser. 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 statistic information you need to set the ShowStats parameter to true for the configuration servlet. To view the information load `http://server_name/servlet_location/HODConfig/info` in your browser.

Related topics:

- [Using Host On-Demand with firewalls](#)
- [Changing the Service Manager port](#)

Configuring Host On-Demand with an IBM firewall



In order for your Host On-Demand services to operate correctly through the IBM SecureWay/Ethernet firewall, you must have the following rules in your filters.cfg file:

From The World to The World, set the source port to greater than 1023. Set the destination equal to 8999. Set TCPIP acknowledgement. Restrict the IP addresses to specifics. For example:

```
# Between The World and The World
# Service : HOD3
# Description : HOD3
permit 0 0 0 0 tcp gt 1023 eq 8999 both both both l=n f=y
permit 0 0 0 0 tcp/ack eq 8999 gt 1023 both both both l=n f=y
```

From Secure Client to The World (using direct outs), set the source port to greater than 1023. Set the destination port equal to 8989. Set TCPIP acknowledgement. For example:

```
# Between Secure Client and The World
# Service : hod2
# Description :
permit 10.10.10.1 255.255.255.255 0 0 tcp gt 1023 eq 8989 both both both l=n f=y
permit 0 0 10.10.10.1 255.255.255.255 tcp/ack eq 8989 gt 1023 both both both l=n f=y
```

From The World to The World (the direct out for the Telnet sessions), use the following code as an example:

```
# Between The World and The World
# Service : Telnet direct out
# Description : Permit Telnet outbound from secure network to non-secure network
permit 0 0 0 0 tcp gt 1023 eq 23 secure route inbound l=n f=
permit 0 0 0 0 tcp gt 1023 eq 23 non-secure route outbound l=n f=y
permit 0 0 0 0 tcp/ack eq 23 gt 1023 non-secure route inbound l=n f=y
permit 0 0 0 0 tcp/ack eq 23 gt 1023 secure route outbound l=n f=y
```

From Secure Client to The World (the HTTP ports for direct out), use the following code as an example:

```
# Between Secure Client and The World
# Service : HTTP direct out
# Description : Permit HTTP from secure network directly to non-secure network
permit 10.10.10.1 255.255.255.255 0 0 tcp gt 1023 eq 80 secure route inbound l=n f=y
permit 10.10.10.1 255.255.255.255 0 0 tcp gt 1023 eq 80 non-secure route outbound l=n
f=y
permit 0 0 10.10.10.1 255.255.255.255 tcp/ack eq 80 gt 1023 non-secure route inbound
l=n f=y
permit 0 0 10.10.10.1 255.255.255.255 tcp/ack eq 80 gt 1023 secure route outbound l=n
f=y
```

Configuring Telnet-negotiated security



Telnet-negotiated security can be configured in the session configuration properties on the server or on the client workstation.

 If **Enable Security** is set to **No**, **Telnet-negotiated** cannot be selected.

On the server:

1. Open the administration window.
2. Click the **Users** tab to open the list of defined groups and users.
3. Select a user or group and click **Sessions** to open the **Configured Sessions** window.
4. If you are creating a new session, click the appropriate button. If you are changing a session, right-click the session icon, then click **Properties**.
5. Click the **Security** tab.
6. Set **Enable Security** to **Yes**.
7. Click **Yes** for **Telnet-negotiated**.
8. Click **OK**.

On the client:

1. Right-click the session icon, then click **Properties**.
2. Click the **Security** tab.
3. Set **Enable Security** to **Yes**.
4. Click **Yes** for **Telnet-negotiated**.
5. Click **OK**.

Related topic:

- [Telnet-negotiated security](#)
- [Telnet-negotiated security overview](#)
- [TLS Protocol Version 1.0](#)
- [How TLS and SSL security work](#)
- [Configuring TLS and SSL](#)

Configuring TLS and SSL

If you have clients outside your firewall connecting to any telnet server or Host On-Demand Redirector inside your firewall, you should configure TLS and SSL connections to ensure your data is secure. To configure TLS and SSL for servers and clients:

1. [Obtain or create certificates for servers](#)
2. [Make server certificates available to clients](#)
3. [Configure clients to use client authentication](#)
4. [Obtain or create certificates for clients needing to provide client authentication.](#)

Related topics:

- [How TLS and SSL security work](#)
- [Examples of when to use TLS or SSL](#)

Disabling Functions: Connection



Items on the Connection tab are associated with sessions. These items appear in the menu when a user right-clicks on a session icon in the Configured Sessions or Active Sessions area of the Client window and in a session window. Active sessions are sessions that have been started but not necessarily connected.

Functions

Select the connection functions for this user:

Run the Same

Starts a session and connects to the host using the same properties as the selected session. Run the Same appears on the menu in the Active Sessions area and on the File menu in the session window.

Allow Connect

Connects an active session. Connect appears on the menu in the Active Sessions area and on the Communication menu of the session window. If you disable this option, make sure Auto-Connect is set to Yes in the session properties window.

Allow Disconnect

Disconnects a session but does not close the session window. Disconnect appears on the menu in the Active Sessions area and on the Communication menu of the session window.

Start Sessions

Starts a session and connects to the host. Start Session appears on the menu of the Client window and the Add Sessions window. Sessions configured to start automatically are not affected by this option. If you disable this option, make sure Start automatically is set to Yes in the session properties window, or else the user will not be able to start a session.

Close Sessions

Closes the session window of an active session. If the session is connected, Close disconnects the session and closes the window. Close appears on the menu in the Active Sessions area of the Client window and on the toolbar of the session window.

View Security

Displays security information for a session. The Security Information window also allows the user to view client certificates. Security appears on the Communication menu in a session window.



This function does not apply to Screen Customizer sessions.

Jump to Next Session

Switches to the next active session. JumpNext appears on the File menu and the toolbar of a Session window.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topic

- [Disabling functions](#)

Setting up a new connection



To open a connection using the default settings:

1. Click Connect to Host.
2. When the logon window appears, logon to the host computer to begin your Host On-Demand session.

To set up and open a connection to a remote computer, you can use the default (preset) Host On-Demand settings, or you can change them to the settings that you prefer. If you use the default settings, make sure the address of the remote computer to which you want to connect is correct. This is the address that appears in the **TN3270E server** field.

If you are not sure what the correct address is for your remote computer, check with your network administrator.

Using Session 1 to bypass logon and start a configured session

- Session1 and session2 do not support new functions added to Host On-Demand Version 5.0. Use the [Deployment Wizard](#) instead.
- These steps require you to have a session already configured. Make sure that the session works correctly before you create the HTML file.
- The user's account must be configured on the Host On-Demand server.
- If you create files for several users, each file must have a different name.
- Launching a pre-configured session using the session1.html file does not let you save preferences. When you close the session, any changes you made are discarded.



To create an HTML file for a user:

1. Open session1.html with an ASCII text editor. Session1.html includes all the possible parameters and can be found in the **doc/samples/html** directory.
2. Add or change the [parameter](#) values.
3. Save your changes and copy the file to the Web server published directory or the On-Demand Server published directory.
4. Test the file to verify that it works correctly.

Using Session 1 and Session 2 to create buttons for sessions

The session1 example uses a configured session. You can use the same steps to create a file that displays sessions as push buttons instead of icons. The example that follows has buttons for 4 sessions in one row. The width and height have been adjusted, but you can use any values.

```
<APPLET archive="hod40.jar" CODE="com.ibm.eNetwork.HOD.SessionLauncher.class"
WIDTH=300 HEIGHT=50>
  <PARAM NAME=CABBASE                               VALUE=hod40.cab>

  <PARAM NAME="User "                                VALUE="orders" >
  <PARAM NAME="Password "                             VALUE=" " >
  <PARAM NAME="Embedded "                             VALUE="false" >
  <PARAM NAME="Rows "                                 VALUE="1" >
  <PARAM NAME="Columns "                              VALUE="4" >
```

Creating a new host session

You can start another host session in any of these ways:

- In an existing session, click File > Run the Same.
- In an existing session, click Same on the toolbar.
- In the Configured Sessions area of the Host On-Demand Applet window, double-click the session icon.

Screen tab



[Screen Customizer](#)

[Font Name](#)

[Font Style](#)

[Cursor Style](#)

[Show Border](#)

[Light Pen Mode](#)

[Show OIA](#)

[Keypad](#)

[Toolbar](#)

[Toolbar Text](#)

[Status Bar](#)

[Confirm on Exit](#)

[Macro Manager](#)

[Graphic Display](#) (printer session)

[Show PA1 Key](#) (3270 printer session)

[Show PA2 Key](#) (3270 printer session)

[Lock](#)

Screen Customizer

Enables or disables Screen Customizer:

- Click Enabled or Client if you want to use a graphical interface.
- Click Administrator if you are using Screen Customizer Administrator and want to customize a graphical interface.
- Click Disabled if you do not want to use a graphical interface.

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

Choose Plain, Italic or Bold.

The default is Plain.

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.

Show Border

Determines whether a border around each protected and unprotected area is displayed. This is the line spacing on a session screen.

The default is Yes.

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).

Show OIA

Determines whether the [Operator Information Area \(OIA\)](#) is visible on the screen.

The default is Yes (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).

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.

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).

Graphic Display (printer session only)

A printer session displays a window that includes several items of information, and shows the printer, workstation and host system as icons. If you turn Graphic Display off, the icons do not display but the other information remains; the window is therefore smaller.

Show PA1 Key (3270 printer session only)

Choose whether to have a button on the screen for the Program Attention 1 key. The function of the key depends on the host application.

The default is No.

Show PA2 Key (3270 printer session only)

Choose whether to have a button on the screen for the Program Attention 2 key. The function of the key depends on the host application.

The default is No.

Lock

Check Lock to prevent users from changing the associated startup value for a session. Users can not change values for most fields because the fields are unavailable. However, functions accessed from the session menu bar or tool bar can be changed.

Customizing Client window icons



You can customize the default icons that Host On-Demand uses for sessions in the Client window. To customize the default session icons:

1. Export an existing Host On-Demand session either from the client or the server. Refer to [Exporting sessions](#) in the online documentation for more information.
2. Open the resulting *.hod file in a text editor.
 - To customize how the session looks in the Client window when it is the selected session, change the name of the graphic file the `selectedImage` parameter refers to.
 - To customize how the session looks in the Client windows when it is not the selected session, change the name of the graphic file the `unselectedImage` parameter refers to.



You must place your graphic files in the `HOD\images` directory.

Save your changes to the *.hod file.

3. Import the *.hod file using the client or the server. Refer to [Importing sessions](#) in on-line documentation for more information.

Customizing hodpdt.list and hodmodel.list

[Customizing hodpdt.list](#)

[Customizing hodmodel.list](#)

Clients running on Windows workstations only can use a locally installed printer driver to print host files. Host On-Demand uses a list file called *hodpdt.list* to identify a local Windows printer with a Printer Definition Table (PDT) file for a 3270 session, and a *hodmodel.list* file with a Printer Model for a 5250 session. Sample *hodpdt.list* and *hodmodel.list* files are provided in the *samples\prt* directory, and must be copied to the *HOD* directory before Host On-Demand can access them. PDT and Model files are provided in the *HOD\pdfpdt* directory. See the [Host Printing Reference](#) for more information about PDT and Model definitions, samples and instructions for customizing these files.

When a 3270 printer session is configured to use the native printer driver on a Windows platform and not to use a PDT, the *hodpdt.list* is not used. When editing the *hodmodel.list* and *hodpdt.list* files you must enter PDT and model names **exactly** as they appear in the PDT or model field of the Printer tab. The PDT and model fields are translated, so the *hodpdt.list* and *hodmodel.list* files must be in the same language as the Host On-Demand clients that are trying to use the Select Printer function. There can only be one set of printer selection list files on a Host On-Demand server, so all the clients using the Select Printer function must be in the same language as the list files.



Customizing hodpdt.list

The *hodpdt.list* file is an ASCII text file that contains a list of names of Windows printer drivers and associated PDT names. The file also contains a default PDT specification to be used when Host On-Demand cannot locate a PDT for the specified Windows printer driver. You can add or change entries in the *hodpdt.list* file using an ASCII text editor.

Sample *hodpdt.list* file:

```
## Print Drivers and associated 3270 PDTs ## This file should contain one or more entries like the following: ##
printerDriverName=3270PDTName ## This file may also contain one optional entry like the following: ##
DEFAULT_PRINT_PDT=default3270PDTName # DEFAULT_PRINT_PDT=Basic ASCII text mode IBM 3130 02D PS
Printer=IBM PPDS Level 2 IBM InfoPrint 20 PCL=HP PCL Level 3 (Laser Printers) Net-It-Now Driver=Basic ASCII text
mode
```

In this example, if Host On-Demand cannot match the specified Windows printer driver with a PDT, the default printer PDT (DEFAULT_PRINT_PDT) that is used is *Basic ASCII text mode*. The printerDriverNames must contain the same white space and punctuation characters that appear in the printer driver names displayed on the Windows workstation. To determine the Windows printer driver name, click Start > Settings > Printers to display the icons of the printers installed on the workstation. Then right click on the printer icon and select properties. The name of the printer is listed first on the General tab. The 3270PDTNames must also contain the same white space and punctuation characters that appear in the Printer Definition Table field on the Printer tab in the 3270 printer notebook.

Customizing hodmodel.list

The *hodmodel.list* file is an ASCII text file that contains a list of names of Windows printer drivers and associated printer model names. The file also contains a default model specification to be used when Host On-Demand cannot locate a model for the specified Windows printer driver. You can add or change entries in the *hodmodel.list* file using an ASCII text editor.

Sample *hodmodel.list* file:

```
## Print Drivers and associated 5250 printer models ## This file should contain one or more entries like the following: ##
# printerDriverName=5250ModelName ## This file may also contain one optional entry like the following: ##
DEFAULT_PRINT_MODEL=default5250ModelName # DEFAULT_PRINT_MODEL=HP LaserJet Series II IBM 3130 02D
```

PS Printer=IBM 3130 Advanced Function Printer IBM InfoPrint 20 PCL=IBM InfoPrint 20

In this example, if Host On-Demand cannot match the specified Windows printer driver with a Model, the default printer model (DEFAULT_PRINT_MODEL) that is used is *HP LaserJet Series II*. The printerDriverNames must contain the same white space and punctuation characters that appear in the printer driver names displayed on the Windows workstation. To determine the Windows printer driver name, click Start > Settings > Printers to display the icons of the printers installed on the workstation. Then right click on the printer icon and select properties. The name of the printer is listed first on the General tab. The 5250ModelNames must also contain the same white space and punctuation characters that appear in the Printer Model field on the Printer tab in the 5250 printer notebook.

Related topic:

- [Host Printing Reference](#)

Database On-Demand HTML table settings

This window is used to configure the various attributes of the HTML table tag and to determine how the HTML file is generated.

Database On-Demand supports the writing of query results in HTML using an HTML template file. A template is an HTML document that contains special tags indicating where the query results should be imbedded. The resulting Web page contains everything in the template file, including the query results in the specified location.

[Table Alignment](#)

[Maximum Table Size](#)

[Equal Column Widths](#)

[Include Border](#)

[Cell Spacing](#)

[Cell Padding](#)

[Table Width](#)

[Include Caption](#)

[Include Column Headings](#)

[Use HTML File As Template](#)

[Template Tag](#)

[Table Text Settings](#)

Table Alignment

Specifies how the table is aligned in the HTML file.

Maximum Table Size

Specifies the maximum number of rows the table can contain. If the maximum number of rows is exceeded, additional HTML files are generated, and forward and backward links are created to link the documents together.

Equal Column Widths

Makes all the columns in the table an equal width. This works only for Netscape Navigator.

Include Border

Creates a border. Border widths are specified in pixels. A border width of 0 is the same as deselecting this option.

Cell Spacing

Specifies the cell spacing for the HTML table. Cell spacing is the thickness, in pixels, of the horizontal and vertical dividing lines that appear between the cells. If deselected, default cell spacing is used. Default cell spacing is dependent upon the individual browser.

Cell Padding

Specifies the cell padding for the HTML table. Cell padding is the amount of space, in pixels, between the cell's border and the text that appears in the cell. If deselected, default cell padding is used. Default cell padding is dependent upon the individual browser.

Table Width

Specifies a desired width, either as a percentage of the display window or as an absolute width in pixels.

Include Caption

Specifies a caption for the table. Type the caption text you want displayed in the text box. The settings button is enabled when this option is selected. The settings window allows configuration of the caption text.

Include Column Headings

Places column headings in the first row of the table. The settings button is enabled when this option is selected, and allows configuration of the column heading text.

Use HTML File As Template

Specifies the HTML file used as the template file. If a template file is not specified, a default HTML file is generated that contains the document tags and the resulting table.

Template files are used to imbed the resulting table in an existing HTML document. The template file is not modified. The output file contains everything from the template file, including the results table at the specified location.

The browse button is enabled when this option is selected, and allows for file browsing.

Template Tag

Specifies where in the template file the table will be imbedded. Use this to customize the tag. This is enabled only when Template File is selected.

Table Text Settings

Displays the window that allows you to set the data text attributes in the table.

OK

Applies the settings for the window and exits.

Cancel

Exits the window without applying the settings.

Database On-Demand save results



Allows you to specify where and how the query result is written.

File Name

The name of the output file.

Browse

Displays the file browse window.

File Type

Specifies how the file should be written. Select one of the file types from the list.

Settings

Displays the HTML table settings window. This is enabled only if HTML file type is selected.

Overwrite File If File Exists

Overwrites the file if the file already exists. A new file is created if it doesn't exist.

Append To File If File Exists

Appends to the file if the file already exists. A new file is created if it doesn't exist. This is enabled only if the file type is ASCII Text or comma-separated variable types.

OK

Applies the settings and exits the window.

Cancel

Exits the window without applying the settings.

Database On-Demand table text settings

Allows you to change the text attributes for the cell data in the table.

Row Alignment

Defines the vertical alignment of each row.

Align Text Data

Defines horizontal text alignment.

Align Numeric Data

Defines numeric data horizontal alignment.

Text Size

Defines the size of the text within the table.

Text Style

Specifies the style of the text within the table. Any number of styles can be selected.

OK

Applies the settings and exits the window.

Cancel

Exits the window without applying the settings.

Database tables



The following SQL statement types are defined:

- **Select**
Allows you to generate SQL queries that contain all rows that match the specified conditions, even if the rows are duplicates. The queries can be sent to a display or to a file.
- **Select Unique**
Allows you to generate SQL queries that contain all unique rows that match the specified conditions. The queries can be sent to a display or to a file.
- **Insert**
Allows you to generate SQL statements to insert new rows into a database.
- **Update**
Allows you to generate SQL statements to update rows in a database.
- **Delete**
Allows you to delete specified rows from a database.

Depending on the SQL statement type you select, you see only the valid tabs for these types of statements. This table indicates the valid tabs for each type of SQL statement.

	Select	Select Unique	Insert	Update	Delete
Logon	X	X	X	X	X
Tables	X	X	X	X	X
Join	X	X			
Condition	X	X		X	X
Columns	X	X			
Sort	X	X			
Output	X	X			
SQL	X	X	X	X	X
Results					
Insert			X		
Update				X	

The tables in this list are identified by the currently-selected connection alias, as specified in the Database URL field on the Logon tab.

Default keyboard mapping

The following table lists supported Host On-Demand keyboard functions, the default keys they are mapped to, and the types of sessions in which the function is supported.

A supported function is denoted by 'X', along with any special notes that apply to the function. The X -f (Minus Function) indicator will appear in the [Operator Information Area \(OIA\)](#) if you attempt to use a function in a session that does not support that function.

Function	Key Mapping	3270	5250	VT	CICS
Alternate Cursor	Not mapped₁	X	X	X	X
Alternate View(note₆)	Ctrl+F3	X	X		
Attention	Not mapped₁	X	X		X
Backspace	Backspace	X	X	X₂	X
Backtab	Shift+Tab	X	X	X	X
Backtab Word	Ctrl+End	X	X		X
Beginning of Field	Not mapped₁	X			X
Clear	Esc	X	X	X₂	X
Clear	Pause/Break	X	X	X	X
Copy₅	Ctrl+Insert	X	X	X	X
Cursor Down	Down arrow	X	X	X₂	X
Cursor Left	Left arrow	X	X	X₂	X
Cursor Right	Right arrow	X	X	X₂	X
Cursor Up	Up arrow	X	X	X₂	X
Cut₅	Shift+Delete	X	X		X
DBCS Input(note₆)	Not mapped₁	X	X		
Delete Character	Delete	X	X	X_{2,3}	X
Delete Word	Ctrl+Delete	X	X		X
DUP Field	Not mapped₁	X	X		X
Enter	Enter	X	X	X	X
Enter or Reset	Ctrl	X	X		X
End Field	End	X	X	X_{2,3}	X
Erase Field	Not mapped₁	X	X		X
Erase EOF	Not mapped₁	X	X		X
Erase Input	Not mapped₁	X	X		X
Field Exit	Ctrl+Enter		X		
Field Mark	Shift+Home	X	X		
Field Minus	Not mapped₁		X		

Field Plus	Not mapped₁		X		
F1-F9, 11, 12	F1-F9, 11, 12	X	X	X	X
F10	F10	X	X	X	X
F13-24	Shift+F1-12	X	X	X₄	X
Graphic Cursor	Alt+PF12	X			
Help	Not mapped₁		X		
Home	Home	X	X	X_{2,3}	X
Insert	Insert	X	X	X_{2,3}	X
Jump Next Session	Ctrl+Page Up	X	X	X	X
New Line	Shift+Enter	X	X		X
Next Word	Not mapped₁	X			X
PA1	Not mapped₁	X	X		X
PA2	Not mapped₁	X	X		X
PA3	Not mapped₁	X	X		X
Page Up	Page Up	X	X	X_{2,3}	X
Page Down	Page Down	X	X	X_{2,3}	X
Paste₅	Shift+Insert	X	X		X
Previous Word	Not mapped₁	X			X
Reset	Not mapped₁	X	X	X	X
Rule	Ctrl+Home	X	X	X	X
SO/SI Display(note₆)	Ctrl+F1	X	X		
System Request	Not mapped₁	X	X		X
Tab Field	Tab	X	X	X₂	X
Tab Word	Ctrl+Page Down	X	X		X
Test Request	Ctrl+F12		X		

1. This function is not mapped to any key but can be mapped to a supported key.
2. VT supports this function but it is up to the host application to act on it.
3. Supported in VT220 mode only.
4. VT supports function keys F1 through F20.
5. The function is only available under browsers that support version 1.1 or higher of the Java Virtual Machine (JVM).
6. The function is available only in a DBCS session.

Default shortcut keys

To access functions that are often used, the following default shortcut keys are available.

Function	Shortcut key
JumpNext	Ctrl+J
Print Screen	Ctrl+P
Exit	Ctrl+Q
Cut	Ctrl+X
Copy	Ctrl+C
Paste	Ctrl+V
Select All	Ctrl+A
Send File to Host...	Ctrl+S
Receive File from Host...	Ctrl+R
Play Macro	Ctrl+M
Run Applet	Ctrl+U
Index	Ctrl+H




Ctrl-key values are sent to the host in VT sessions, not to the session. The default values for the menu functions have been removed from VT sessions, so that the appropriate values are sent to the host. You can use the [Keyboard Remap](#) function to map these menu functions to other keys.

Related topics


- [Remapping the keyboard](#)
- [Default characters and functions](#)
- [Thai shortcut keys](#)
- [BIDI shortcut keys](#)

Default shortcut keys

To access functions that are often used, the following default shortcut keys are available.

 Because menu items and shortcut keys can be remapped using the [Keyboard Remap](#) function, shortcut keys might be different than what is listed here.

Function	Shortcut key
JumpNext	Ctrl+J
Print Screen	Ctrl+P
Exit	Ctrl+Q
Cut	Ctrl+X
Copy	Ctrl+C
Paste	Ctrl+V
Select All	Ctrl+A
Send File to Host...	Ctrl+S
Receive File from Host...	Ctrl+R
Play Macro	Ctrl+M
Run Applet	Ctrl+U
Index	Ctrl+H

 Ctrl-key values are sent to the host in VT sessions, not to the session. The default values for the menu functions have been removed from VT sessions, so that the appropriate values are sent to the host. You can use the [Keyboard Remap](#) function to map these menu functions to other keys.

Related topics

- [Thai shortcut keys](#)
- [BIDI shortcut keys](#)



Edit Existing HTML File

Use this panel to choose an HTML file to edit.

The Deployment Wizard can only edit HTML files previously created by the wizard. Attempting to edit a file that was not created by the Deployment Wizard will corrupt the file and cause unpredictable results.



File Name and Output Format

Page Title

Specify the title of the HTML file. This appears in the title bar of the browser window.

This does not apply to portlets.

File Name

Specify the name of the HTML file, the zip file, and/or the portlet to create. Select Browse to change the directory.

In order to support clients whose computers have file systems that do not handle file names greater than eight characters (such as FAT-16), it is recommended that you keep the names of your Web pages to eight characters or less. A computer with this type of file system will not be able to run local preference Web pages that have names greater than eight characters.

The default directory for a full Host On-Demand installation is the Publish directory. For a standalone Deployment Wizard installation, the default is the root directory on the drive where the Deployment Wizard is installed.

Directory

Select the output directory for the HTML file, the zip file, and/or the portlet.

Output

Select one or more of the following output formats:

Output HTML

Creates the set of Deployment Wizard-generated files. This format is required for use by the Web server. (Recommended if you are using the Deployment Wizard on your Host On-Demand server machine.)

Output Zip

Creates a zip file of the Deployment Wizard-generated files. This format is required for use with DWUnzip, which is a tool that runs on the Host On-Demand server that can be used to install the Deployment Wizard-generated files. Refer to [Using DWunzip](#) for more details about DWunzip. (Recommended if you are not running the Deployment Wizard on your Host On-Demand server and will need to move the created files to another server.)

Output Portlet

Creates a portlet for Portal Server. For an overview of how to use Host On-Demand as a portlet, refer to the [Using Host On-Demand Clients with Portal Server](#) section in the Planning, Installing, and Configuring Host On-Demand guide.

If you choose Output Portlet option, you will need to configure additional parameters.

PAR vs WAR: Portal Server requires portlets to be in a portlet archive (PAR) file format for versions 2.1 and earlier. For versions 4.1 and later, Portal Server requires portlets to be in a web application archive (WAR) file format. The default format is PAR. Refer to the [WebSphere Portal Server Web site](#) for details.

Portlet Details: This button contains the following optional fields that may be configured for the Host On-Demand portlet. The default portal locale is the same as the system locale that is used when running the Deployment Wizard, and the values of that locale are displayed. Note that the Portal administrator may change these fields once the portlet has been installed.

Title: Specify a title for the portlet.

Short Title: Specify an abbreviated title for the portlet.

Description: Provide a description of the portlet.

Keywords: Provide keywords associated with your portlet.

HOD Server URL: Because the Host On-Demand portlet runs within Portal Server, the Portal Server needs to be able to locate the Host On-Demand Server. The URL that you specify here must identify the Host On-Demand publish directory. An example HOD Server URL is *http://server_name.mycompany.com/hod*, where *server_name* is the name of the server where Host On-Demand is installed. You are not required to enter a value for this field since it can be modified by a Portal Server administrator once the portlet has been installed. This field is a configuration parameter of the generated portlet and is named `hodCodeBase`.

Summary

Shows the major Deployment Wizard options that were selected for this HTML file/zip file/portlet. Click Details to view all the options selected. To see DBCS in the detail dialogue comments, make sure you are using an editor program that supports UTF-8 encoding.



Logon Type

Choose how users will access the Host On-Demand configuration server.

Prompt users to enter Host On-Demand user ID

Users will be prompted to enter their user ID and password when starting this file.

Automatically log users on to Host On-Demand using Windows username

Users must be logged on to a Windows domain to use this option. The Host On-Demand logon panel will not be displayed and the Windows username will be used as the Host On-Demand user ID.

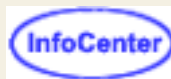
Users are from Windows domain

Users must be from this Window's domain or they will be denied access to Host On-Demand. You can specify multiple domains by listing all the domains separated by commas.

Create user ID if it doesn't exist?

If you choose yes, and the Host On-Demand user ID doesn't already exist (matching the Window's username), one will automatically be created in the specified Host On-Demand group. (Unless you are using LDAP, you can add the user ID to multiple groups by listing all the groups separated by commas.) If you choose no, and the user ID doesn't already exist, they will be denied access to Host On-Demand.

Disable Functions: File Transfer



The File Transfer tab enables access for transferring files to and from zSeries or iSeries systems using Host File Transfer.

Functions

Select the file transfer functions for this user:

Receive Files from Host

Receive, or get, files from the host. Receive files from host appears on the Action > Transfer Files menu and on the toolbar in a 3270 or 5250 display session window, when the File Transfer Type is Host File Transfer.

Send Files to Host

Transfer, or send, files to the host. Send files to host appears on the Action menu > Transfer Files and the toolbar in a 3270 or 5250 display session window, when the File Transfer Type is Host File Transfer.

Change File Transfer Defaults

Changes the default values for text or binary send and receive options. It also set values for options such as transfer mode and the PC code page. File Transfer Defaults appears on the Action menu and the Edit > Preference menu in a 3270 or 5250 display session window.

Launch FTP Session

Launches an FTP session by clicking an icon on the host session toolbar and by selecting Actions > Transfer Files on the session menu.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topic

- [Disabling functions](#)

Disabling Functions: Macro

A macro is a sequence of commands that performs actions on the host. Macros can be used for complex or simple tasks that you do often. Recording a macro can prevent user errors and makes a task quick and easy to perform. All macro functions are accessed from the display session window only.

Macros configured to start automatically are started even when Play Macro is disabled.



Functions on this tab do not apply to Screen Customizer sessions.

Functions

Select the macro functions for this user:

Play Macro

Plays a macro. Play macro appears on the session toolbar, the Macro Manager toolbar, and on the Action menu.

Edit Macro

Opens the Macro Editor so that you can modify or create a macro. The Edit Macro button appears on the Macro Manager toolbar. The Macro Manager must be enabled to use this function.

Delete Macro

Deletes a macro from the Macro Manager macro list. Delete macro appears on the Macro Manager toolbar. The Macro Manager must be enabled to use this function.

Record Macro

Records a new macro and saves it in the Macro Manager macro list. Record Macro appears on the session toolbar, the Macro Manager toolbar, and the Action menu.

Toggle Macro Manager State

Displays the Macro Manager toolbar where you can record, play, and edit macros. Macro Manager appears on the toolbar and the View menu.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topics

- [Macro Manager](#)
- [Disabling functions](#)

Disabling Functions: Other



Functions

Select the functions for this user:

Cut/Copy/Paste

Uses the clipboard functions in a display session. Cut, copy, and paste appear on the Edit menu and the toolbar of a session window.

Print Screen

Prints a screen to a printer installed on your desktop. Print Screen appears on the File menu and the toolbar of a display session window.

Print Screen Setup

Provides Page Setup (paper type, orientation, and margins) and Print Setup (header/footer). Print Screen Setup appears on the File menu, and Page Setup and Print Setup appear on the toolbar of a session window.

Toggle Light Pen Mode

Switches light pen mode on or off in a 3270 or CICS display session. If you switch light pen mode on, you can use your mouse as a light pen. Light-pen mode appears on the View menu and the toolbar of a session window.

Help

Provides access to the online help. This disables the session window Help menu and the Help buttons on all product windows.

Edit BIDI Options

Provides bidirectional language support (Arabic and Hebrew). BIDI options are set on the Language tab when configuring a display session.

Edit Thai Options

Provides Thai language support. Thai options are set on the Language tab when configuring a display session.

Run Applet

Loads and runs a user-defined applet. Run Applet appears on the Action menu and the toolbar of the session window. Applets will still run if they are configured to Auto-Start in the session properties window. This option applies to display sessions only.



Edit BIDI Options and Edit Thai Options do not apply to Screen Customizer sessions.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topic

- [Disabling functions](#)

Disabling Functions: Printer



Items on the printer tab provide functions that are accessed from the 3270 printer session menu.



Functions on this tab do not apply to Screen Customizer sessions.

Functions

Select the Printing functions for this user:

Graphic Display

Turns the graphic display on or off. The graphic shows icons that represent the printer-to-host connection. Graphic Display appears on the View menu of the printer session window.

Print Test Page

Prints a test page. Print Test Page appears on the File menu of the printer session window.

Eject Page

Ejects a page from the printer. Eject Page appears on the File menu of the printer session window.

Page Properties

Opens the Page Properties window (defines the page layout). Page Properties appears on the File menu of the printer session window.

Printer

Opens the Printer window (defines the printer to be used). Printer appears on the File menu of the printer session window.

Cancel Job

Cancels the job currently being sent to the host. Cancel Job appears as a button on the bottom of the printer session window.

PA1

Displays a Program Attention 1 key, displayed as a button, if the host application program has defined one. The PA1 key provides a means of communicating with the host application program.

PA2

Displays a Program Attention 2 key, as a button, if the host application program has defined one. The PA2 key provides a means of communicating with the host application program.

Settings

Select a setting for each function:

Enabled

Allows group or user to access this function.

Enable All

Enables all the functions listed on the current screen.

Disabled

Does not allow group or user 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..

Related topic

- [Disabling functions](#)

Using Session 1 and Session 2 to disable functions

To disable graphical interface functions, use the [Disable Function](#) accessed from the Administration window or the [Deployment Wizard](#).

Not only can you provide Host On-Demand functions in a customized HTML file, but you can also create an HTML file that starts a session with some functions disabled. To do this, add the Disable parameter to the <APPLET> tag in the HTML file.

For example, to disable the Cut/Copy/Paste function, add the following:

```
<PARAM NAME=Disable          VALUE= "CUTPASTE" >
```

You can disable more than one feature by separating the values with semicolons. For example, to disable the Cut/Copy/Paste, 5250 Emulation, and Macro Record/Play features, add the following:

```
<PARAM NAME=Disable          VALUE= "CUTPASTE ; EMUL5250 ; MACRO" >
```

The following functions can be disabled:

Parameter Value	Function
CLRMAP	Color remapping
CUTPASTE	Cut/copy/paste
EMUL3270	3270 session
EMUL5250	5250 session
EMULCICS	CICS gateway session
EMULVT	VT session
FILEXFER3270	3270 file transfer
FILEXFER5250	5250 file transfer
EMUL3270PRT	3270 printer session
EMUL5250PRT	5250 printer session
KEYMAP	Keyboard remapping
MACRO	Macro record/play
SSL	Security
USERAPPLET	Startup-applets and run applet

Related topics

- [Disabling graphical interface functions](#)

Editing macro links



Allows you to select the order of the defined screens.

To change the order of the defined screens:

1. Click Macro Manager on the toolbar.
2. Select a macro from the list.
3. Click Edit.
4. Click the Links tab and select a screen from the Screen Name list.

For each screen, the Links tab shows which other screens are Valid Next Screens. This limits what screen definitions the macro will use when identifying subsequent screens. For example, after identifying Screen1 and performing the defined actions, to identify the next screen that appears, the macro will only compare it to the Valid Next Screens for Screen1. Only screens in the Valid Next Screens list can be a "match". By limiting the set of screens that the macro uses to identify the next screen, this lessens the chance of having multiple "matches" for screens with similar identifiers. By default, when Macro Manager records a macro, for a given screen, the following screen will be the only Valid Next Screen.

All of the screens defined in the macro are listed in the Screen Name list. Select a screen from the Screen Name list. To identify the valid next screens for this screen, choose the screen from the Available Screens list. Click the right arrow to move the screen to the Valid Next Screens list. To remove a screen from the Valid Next Screen list, select the screen and click the left arrow to move the screen back to the Available Screens list.

The Timeout value is the time to wait between screens. The value you set for a screen here overrides the value set for all screens on the Macro tab.

Related topics

- [Using the Macro Editor \(an overview\)](#)
- [Editing the XML script](#)
- [Importing a macro](#)
- [Exporting a macro](#)



EHLAPPI for Host On-Demand enablement tool

The EHLAPI for Host On-Demand enablement tool allows users to run existing EHLAPI applications using a variety of interfaces on Host On-Demand emulator sessions. For details about the supported interfaces and environments and installation instructions, as well as a complete list of the known limitations, see the Readme.

Both the tool and the accompanying Readme file are available on the IBM Software Internet Service Delivery site at <http://www6.software.ibm.com/aim/home.html> on the Host On-Demand CSD page under Tools and Utilities. If this is your first time at the site, you need to register.

VT 420 emulation limitations



VT 420 emulation limitations are contained in the following areas:

Not Implemented

The following VT 420 features are not implemented:

- Display Controls Mode
- Keyboard Layout and Control
- Printer Port Control Functions
- Device Status Report (DSR)
- Terminal State Reports
- Presentation State Reports
- Mode Settings
- Control Function Settings
- Window Reports
- User-Preferred Supplemental Set
- PC Term Mode

Keyboard

Some local function keys cannot be enabled or disabled in Host On-Demand VT sessions, and menu keys that are mapped to menu commands are not available as local function keys. These functions include:

- Ctrl+C is not available for mapping copy to clip board
- Ctrl+A is not available for select (Mark) item

The following VT modifier keys are not visible to Host On-Demand VT sessions:

- Left Shift
- Right Shift
- Lock
- Left Alt Function
- Right Alt Function
- Left Compose Character
- Right Compose Character

The DECEKBD report is not supported due to technical limitations regarding the determination of the state of the keys on the keyboard.

Due to limitations in Java keyboard handling, Host On-Demand does not map by default the numeric keypad keys so that they can differentiate between numeric mode and application mode.

Character Set

All characters in the terminal screen must be stored as Unicode values. The following character sets contain characters that can not be matched to a Unicode value:

Character Set	Position
Dec Technical Character set	2B, 2C, 2D, 2E, 2F, 30, 31, 32
PC Multilingual/International - Left Side	08, 17
PC Multilingual - Right Side	9B
PC Spanish	A9, AA

Host On-Demand does not support the use of Raster fonts for VT emulation. VT emulation is dependent on the Java Virtual Machine's available set of fonts for rendering the VT terminal screen. Each operating system and browser combination is missing some of the characters contained in a few of the new character sets. The number of non-renderable characters and their positions varies by operating system and browser, so they are not listed here.

Enabling host graphics (3270)



To enable host graphics:

1. Open the client window.
2. Right-click the session for which you want to enable host graphics, then click Properties.
3. Click Advanced.
4. Click Yes to enable Host Graphics.
5. Select a [Character cell size](#).
6. Click OK.



Host On-Demand does not support retained-mode redraw of host graphics. If you resize the screen, press Clear to redraw the graphics portion of the screen. (This command is application-dependent, but Clear usually works.)

Related topics

- [Graphics function comparison](#)
- [Graphics order list](#)



Overwrite existing file?

Select OK to overwrite the existing file and replace it with the exported session. If you choose to overwrite, you cannot recover the contents of the original file.

Select Cancel to return to the Export Session window without saving the exported file.

Recording an express logon macro



Application ID

This name must match the RACF PTKTDATA (Passticket Data Profile) application name that is configured on the OS/390 V2R10 host. This name could be the same as the application name that the user is logging onto (for example, the name on USSMSG10). When creating PTKTDATA profiles for applications such as TSO, the application name portion of the profile will most likely not be the same. For example, RACF requires that the application ID portion of the profile name be TSO+SID. Refer to OS/390 V2R10.0 SecureWay Security Server RACF Security Administrator's Guide to determine the correct profile naming. If using TSO Generic Resource names, RACF apar OW44393 is needed. You can obtain this ID from the host administrator.

Screen Criteria

Select a criteria for the macro to record. This window allows you to proceed through the host screens until you reach the screen containing the information needed by the macro to complete the logon.

Is an alternate start screen

The alternate start screen is a screen from which the user might want to play the macro to logon to the application. If the application has more than one possible start screen, you should identify it during the recording process so the macro can be played from that screen. For example, the logon process might begin from the USSMSG10 screen or the application logon screen. You can start the logon macro from either the start screen or the alternate start screen. You can designate only one screen as an alternate start screen. There is no alternate start screen after the screen that contains the user ID.

Contains a user ID field

The screen contains a host user ID field. Only one screen can be identified by a user ID field.

Contains a password field

The screen contains a password field. Only one screen can be identified by a password field.

Alternate Start Screen

Specify whether this screen is an alternate start screen. The macro can start playing when a start screen is recognized or when an alternate screen is recognized. You can have only one alternate start screen and it must be after the start screen.

Wait Conditions

Specify the wait conditions for the macro to use to identify this screen. This setting causes the macro to wait during playback until it recognizes a screen according to conditions that you set. If the macro recognizes the screen within the timeout period, it continues. If it does not, it stops.

Field Count

Total number of fields on the screen.

Input-Field Count

Total number of input fields on the screen (fields that you can type in).

Wait for OIA to become Uninhibited

If checked, the OIA must become uninhibited (no data communication and you are able to enter keystrokes) before the macro continues.

Use Cursor Position

Identifies the screen by the cursor position.

Keyword

Any word that will appear on the screen and that you want the macro to recognize. You should try to choose a word that is unique to that screen.

Timeout

A value in milliseconds (for example, 10000 is 10 seconds). Until all the conditions that you define have been satisfied, the macro will wait for the time specified. If the timeout expires before all the conditions have been met, the macro will stop playing back and display a message telling you the screen on which it failed.

A value less than or equal to zero adds an indefinite wait.

If the macro consistently times out too soon, edit the macro to increase the timeout value.



- If the number of fields in your host application screen varies from time to time, you will sometimes not get a match for the screen recognition. If this happens, re-record the macro without specifying either type of field count.
- The macro function performs automatic screen-recognition by watching the cursor position on each screen. Do not add a Wait Condition for every screen unless you are sure that the cursor is a sufficient way of recognizing a screen.

User ID Field and Location

Select whether this screen contains a user ID field for logging on.

1. Click Current to use the cursor's current position on the session screen if you know it's correct. If not, move the cursor to the beginning of the user ID field on the session screen to identify where the user will enter the user ID and click Current. The field values change to match the new cursor position on the screen. If the initial cursor position is correct then there is no need to move the cursor on the session screen.
2. Enter the user ID in the User ID field on this window, not on the session screen.

Row/Column

Determines the cursor position on the screen for the user ID field.

User ID

You must enter a user ID to continue recording the macro. The macro enters the actual user ID text in the user ID field on the session screen and writes a predefined text string to the macro file as an identifier for the telnet server.

Password Field and Location

Select whether this screen contains a password field for logging on.

1. Click Current to use the cursor's current position on the session screen if it's correct. If not, move the cursor to the beginning of the Password field on the session screen to specify where the user will enter the password and click Current. The field values change to match the new cursor position on the screen. If the initial cursor position is correct then there is no need to move the cursor on the session screen.
2. Enter the password in the Password field on this window, not on the screen.

Row/Column

Determines the cursor position on the screen for the password field.

Password

You must enter a password to continue recording the macro. The macro enters the actual password text in the password field on the session screen and writes a predefined text string to the macro file as an identifier for the telnet server.

Auto-Start Macro

Select whether you want this macro to run automatically when the session is started. If you select Yes then the macro will start playing the next time you start this session.

Numeric Field Lock



When turned on, Numeric Field Lock allows you to type only the characters 0 through 9, -, +, period, and comma into fields defined by a host application as numeric.

Numeric Field Lock is available for 3270 sessions only.

Font



Select a new font, a font style, and a font size.

The Sample window displays your font selection.

Host graphics function comparison



Host On-Demand Host Graphics is designed for functional compatibility with IBM 3179G. This table is a Host Graphics comparison of host graphics function provided by IBM 3270 emulators.

	HOD V4.0	J3270PC	PCOMM WIN16	PCOMM OS/2 or WIN32	CM/2
Screen size:					
Mod2	X	X	X	X	X
Mod3	X	X	X	X	X
Native graphics	X	X	X	X	-
OS/2 LINK	-	-	X	X	X
PSS	-	-	X	X (V4.1)	-
Host print (auxiliary device)	-	X (Plotter)	X (PCLK)	X (OS/2 Link)	X
Graphic local copy	X	X	X	X	-
Multi-session	X	-	X	X	X
Cross hair cursor	-	X	-	X (V4.1)	X
Rubber band/box	-	-	-	X (V4.1)	X
Datakey choice	-	-	-	X (OS/2 Link)	X
Stroke input	-	X	-	-	-
Clipboard (copy)	-	-	X	X	X
DDM PIF to META	-	-	X (PCLK)	X (OS/2 Link)	X
Transparency	X	-	X (Bitmap)	X (Bitmap)	-
Character precision	2	3	1 (Native)	2 (PCLK)	1 (Native) 2 (OS/2 Link)
Graphic Color	16	8	16	16	16
Pattern	16	16	16	16	16
Marker	8	8	8	8	8
Line type	8	8	8	8	8

General help information



To see what a description of each menu button, point at the button and pause. The name of the button appears in the Screen Customizer status bar.

Click in the list below for an explanation of each function.

- [File menu](#)
- [Appearance menu](#)
- [Communication menu](#)
- [Assist menu](#)
- [Print menu](#)
- [Help menu](#)
- [Keypad](#)
- [Toolbar](#)

Menu name	Menu choices	Shortcut	Description
File	Exit	Ctrl+Q	Closes the Active session
View	Toolbar		Toggle switch that shows or hides the toolbar
	Keypad		Toggle switch that shows or hides the keypad
	Hotspots		Toggle switch that shows or hides hot spots
	Menu Buttons		Toggle switch that shows or hides menu buttons
Communication	Connect		Connects to the host session
	Disconnect		Terminates the connection with the active host session
Assist	Font...		Defines the font type, style, and text size for all screens in this application
	Color Remap...		Defines the foreground and background colors for all screens in this application
	Menu Buttons		Defines the appearance of the menu buttons
	Refresh		Updates the active screen to reflect changes made in the Customization Studio
Print	Print Screen		Prints the current host screen
Help	Index		Explains Screen Customizer functions

	About Screen Customizer	Displays this Screen Customizer version number
Keypad (Sends function key commands to the host)	PF1-thru-PF24, Enter, Reset, Clear, Fld+, Fld-, PgUp, PgDn, Fld, FldExt, Attn, SysReq	Host-defined function keys
	Insert	Allows you to work in insert mode
	New Line	Puts the cursor in the nearest input field starting from the new line
	ErsInp	Erases all input from the screen
	ErsFld	Erases all input from the field
	ErsEOF	Erases all the input from the cursor position to the end of the field
	Delete	Sends the delete character that immediately follows the cursor position
	NewPad	Moves to the second keypad row
	FrstInp	Sends the cursor to the first input field on the screen
Toolbar		Shortcut buttons for frequently-used menu options

Screen Customizer/LE



Screen Customizer/LE for Host On-Demand is an alternative graphical user interface, or GUI, that lies over your host application screen and makes it look like a Windows application. It gives the Host On-Demand green screen (the traditional screen with a black background and bright green text) a 3-dimensional look and feel. Many people who are unfamiliar with the green screen find the Screen Customizer/LE GUI more user-friendly and familiar. To use the Screen Customizer Interface, click Enabled for Screen Customizer Interface on the Screen page of the session configuration.

Graphics-order lists



Graphics orders are divided into three groups:

- Output Primitive Orders
- Attribute Setting Orders
- Procedural Instruction Orders

The following tables show the graphics orders supported by IBM 3270 emulators.

Output Primitive Orders	HOD V4.0/ 3192-G	J3270PC	PCLK/OS/2 Link	PCOMM WIN32	PCOMM OS/2
Arc (C6/86)		X			X
Begin Area (68)	X	X	X	X	X
Begin Image (D1/91)	X	X	X	X	X
Character String (C3/83)	X	X	X	X	X
End Area (60)	X	X	X	X	X
End Image (93)	X	X	X	X	X
Fillet (C5/85)	X	X		X	X
Full Arc (C7/87)	X	X		X	X
Image Data (92)	X	X	X	X	X
Line (C1/81)	X	X	X	X	X
Marker (C2/82)	X	X	X	X	X
Relative Line (E1/A1)	X	X	X	X	X

Attribute Setting Orders	HOD V4.0/3192-G	J3270PC	PCLINK/OS/2 Link	PCOMM WIN32	PCOMM OS/2
Set Background Mix (0D)	X	X	X	X	X
Set Character Angle (34)*	X	X			
Set Character Cell (33)	X	X			
Set Character Direction (3A)	X	X	X	X	X
Set Character Precision (39)	X	X			
Set Character Set (38)	X	X			X
Set Character Shear (35)*	X	X			
Set Color (0A)	X	X	X	X	X
Set Extended Color (26)	X	X	X	X	X
Set Line Type (18)	X	X	X	X	X
Set Line Width (19)	X	X	X	X	X
Set Marker Cell (37)	X	X			
Set Marker Precision (3B)	X	X			
Set Marker Set (3C)	X	X			
Set Marker Symbol (29)	X	X	X	X	X
Set Mix (0C)	X	X	X	X	X
Set Pattern Set (08)	X	X			
Set Pattern Symbol (28)	X	X	X	X	X
Set Viewing Window (27)		X			

Miscellaneous Drawing Orders	HOD V4.0/3192-G	J3270PC	PCLINK/OS/2 Link	PCOMM WIN32	PCOMM OS/2
Comment (01)	X	X		X	X
No Operation (00)	X	X	X	X	X
Segment Characteristics (04)	X				

Set Arc Parameters (22)	X	X		X	X
Set Current Position (21)	X	X	X	X	X
End Prologue (3E)	X	X		X	X
End of Symbol Definition (FF)	X				

Procedural Instructions	HOD V4.0/3192-G	J3270PC	PCLINK/OS/2 Link	PC/3270 WIN32	PC/3270 OS/2
Erase Graphic PS (0A)	X	X	X	X	X
Stop Draw (0F)	X	X			
Attach Graphic Cursor (08)	X	X	X	X	X
Detach Graphic Cursor (09)	X	X	X	X	X
Set Graphic Cursor Pos(31)*	X	X	X	X	X
Set Current Defaults (21)	X	X	X	X	X
No Operation (00)	X	X			
Comment (01)	X	X			

*Note: Host On-Demand Version 4.0 accepts these graphics orders, but ignores them.





Viewing status bar history

To see recent status bar messages, click the arrow on the status bar. Status bar messages display connection status messages and are listed in order of occurrence with the most recent messages at the bottom of the list and the oldest messages at the top. The maximum number of messages that can be displayed is 100. Once this number is reached, the oldest messages are deleted and new messages are added.

To change the number of messages displayed in the History window, add the `StatusbarHistorySize` parameter to the client file, for example:

```
<PARAM NAME="StatusbarHistorySize" VALUE="50">
```

In the Status Bar History window:

- Click  to clear all messages from the Status Bar History window.
- Click  to launch the Status Bar History in a separate window, where you can save the status history as a separate file.
- Click  or double-click the selected message for help information about the message. The Help button is enabled only when additional help is available.
- Click  or press Escape to close the Status Bar History window.

Host On-Demand

Host On-Demand provides a number of different clients, each listed on the Getting Started page. You can start the client of your choice simply by clicking its link. The page also includes links to one or more utilities, to Planning, Installing, and Configuring Host On-Demand, and to the readme file.

The purpose of the page is to provide an easy way to start any of the clients without having to know or type its file name. To customize the page, edit the HODMain.html file.

Package	Client	Description	More Help
Administration clients	Administration client (HODAdmin.html)	Starts the administration applet.	Administration clients
	Administration client cached (HODAdminCached.html)	Starts the administration applet that can be accessed without first removing the cached client.	Administration clients
	Administration client cached with problem determination (HODAdminCachedDebug.html)	Starts the administration applet that can be accessed without first removing the cached client. This client also has problem determination capability, allowing logging and tracing of users' sessions. If there is a problem that you cannot resolve, ask the user to load this client instead of the usual one.	Administration clients
Full administration clients	Full administration client (HODAdminFull.html)	Starts the administration applet. This full client enables administrators to modify a user or group session's runtime properties.	Full administration clients
	Full administration client cached (HODAdminCachedFull.html)	Starts the administration applet that can be accessed without first removing the cached client. This full client enables administrators to modify a user or group session's runtime properties.	Full administration clients
	Full administration client cached with problem determination (HODAdminCachedDebugFull.html)	Starts the administration applet that can be accessed without first removing the cached client. This full client enables administrators to modify a user or group session's runtime properties. This client also has problem determination capability, allowing logging and tracing of user or group sessions. If there is a problem that you cannot resolve, ask the user to load this client instead of the usual one.	Full administration clients

Emulator Clients	<p>Cached client (HODCached.html)</p>	<p>Starts the Cached Client and all the available client function, including the Screen Customizer interface. The first time you load this client, all the client components are downloaded and saved into the browser cache on your hard disk; thereafter, the client is loaded from the hard disk unless any components have been updated on the server. If so, only the new components are downloaded automatically.</p>	<p>Cached clients</p>
	<p>Cached client with problem determination (HODCachedDebug.html)</p>	<p>HODCachedDebug.html starts the Cached Client and all the available client function, including the Screen Customizer interface. This client also has problem determination capability, allowing logging and tracing of users' sessions. If there is a problem that you cannot resolve, ask the user to load this client instead of the usual one.</p>	<p>Cached client</p>
	<p>Download client (HOD.html)</p>	<p>Starts the standard client, which includes all the client function except the Screen Customizer interface and ability to do problem determination. This client is downloaded from the server every time.</p>	<p>Download clients</p>
	<p>Download Client with problem determination (HODDebug.html)</p>	<p>Starts the standard client, with the addition of the problem determination capability, allowing logging and tracing of users' sessions. If there is a problem that you cannot resolve, ask the user to load this client instead of the usual one.</p>	<p>Using the Log/Trace Facility</p>
	<p>Function On-Demand (HODThin.html)</p>	<p>Starts a small client. Initially, only the basic files are downloaded. Other files are downloaded as required, according to what functions the configuration specifies or what functions are started while the session is active. For example, if the configuration is for a 3270 display session, only the files needed for this are downloaded, and the files required to remap a key or transfer a file are downloaded only when the function is called for. This client is downloaded from the server every time.</p> <p>This function is not supported with browsers using a Java 2 Runtime Environment.</p>	<p>Function On-Demand client</p>

Database clients	Database On-Demand (HODDatabase.html)	Starts the Database-On Demand client which lets you exchange data between an iSeries database and a workstation application.	Database On-Demand clients
	Database On-Demand client cached (HODDatabaseCached.html)	Starts the Database-On Demand client which lets you exchange data between an iSeries database and a workstation application, and can be accessed without first removing the cached client.	Database On-Demand clients
	Database On-Demand (HODDatabaseCachedDebug.html)	Starts the Database-On Demand client which lets you exchange data between an iSeries database and a workstation application, and can be accessed without first removing the cached client. This client also has problem determination capability, allowing logging and tracing of users' sessions. If there is a problem that you cannot resolve, ask the user to load this client instead of the usual one.	Database On-Demand clients
Utilities	Remove Cached Client (HODRemove.html)	This utility can be used to remove any cached client from a workstation.	Remove Cached Client
	Remove Cached Client(Java 1) (HODRemove.html)	This utility can be used to remove the Java 1 cached client from a workstation.	Remove Cached Client
	New user client (NewUser.html)	This utility can be used by users to create new accounts, if you check Allow users to create accounts on the Users/Groups window.	Enabling users to create accounts
	New user client cached (NewUserCached.html)	This utility can be used by users to create new accounts, if you check Allow users to create accounts on the Users/Groups window, without first removing the cached client.	Enabling users to create accounts
	New user client with problem determination (NewUserCachedDebug.html)	This utility can be used by users to create new accounts, if you check Allow users to create accounts on the Users/Groups window. This client also has problem determination capability, allowing logging and tracing of users' sessions. If there is a problem that you cannot resolve, ask the user to load this client instead of the usual one.	Enabling users to create accounts
Installation Images	Deployment Wizard	Stand-alone Deployment Wizard installation	Installing the Deployment Wizard

Java 2 Runtime Environment

IBM Win32 Java 2 Runtime

[Planning
for Java 2 on the
client](#)

Moving your Host On-Demand server configuration from one server to another

You can move your Host On-Demand server configuration from one server to another. 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 Planning, Installing, and Configuring Host On-Demand 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.

- 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*.
 - 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*.
4. Start the Host On-Demand Service Manager on *server2*.

Unlocking the keyboard



If your keyboard is locked, attempt to put focus on the Host On-Demand window by clicking in the window area under the title bar.

Language Tab



Bidi options

Edit Bidi options

- [Numeral Shape](#) (Arabic)
- [Text Type](#) (Arabic/Hebrew)
- [Text Orientation](#) (Arabic/Hebrew)
- [Round Trip](#) (Arabic/Hebrew 5250/3270)

Display BIDI options

- [Allocate space for LamAlef](#) (Arabic 5250)
- [Text Type](#) (Hebrew VT)
- [Numeral Shape](#) (Arabic VT)
- [BIDI Mode](#) (Arabic VT)
- [Cursor Direction](#) (Hebrew Visual VT)
- [Smart Ordering](#) (Arabic/Hebrew Logical VT)
- [Show Text Attributes](#) (Arabic/Hebrew Logical VT)
- [Print RTL file](#) (Arabic/Hebrew 3270 Printer session)

Thai options

- [Thai Display Mode](#)
- [Lock](#)

DBCS options

- [User Defined Character \(UDC\) Setting](#)
- [UDC Table Selection](#)
- [IME Auto Start](#)

BIDI options

Edit Bidi options

Numeral Shape (Arabic only)

Determines the shape of numeric characters of the string copied to or pasted from the clipboard. Choose 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. Select 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. Select Nominal, National, or Contextual.

The default is Contextual.

Text Type (Hebrew VT only)

Determines the format of the text characters stored. Select 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 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. For more information, see [Printing Right-to-left files](#).

The default is No.

Thai options

Thai Display Mode

Select a display mode:

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

Check Lock to prevent users from changing the associated startup value for a session. Users can not 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

Determine 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.

Using a light pen

Click View > Light Pen Mode to switch light pen mode on or off.

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.

Logging on as a user



1. Open a browser and type in the URL address supplied by the system administrator.
2. Type your user ID and password.
3. If you want to change your password , click the Change password box. You can change your password only if your administrator has allowed this option.
4. Click Log On. A window opens containing two session areas:
 - **Configured sessions**
This area contains an icon for each of the sessions that the administrator has configured for you. To start a session, double-click the appropriate icon. For information about changing or copying a session, click Help.
 - **Active sessions**
When you have started a session, this area contains a lightning bolt and the name and ID of the session.

If you have your own user ID, changes that you make are saved.

If you logged on with a shared user ID, you can change the session parameters that have not been disabled. You can make changes in a host session window, but the changes will be discarded when you log off.

Viewing the server's message and trace log

Click the Server Log to open the Trace/Message Console window. This window displays messages and trace data created by the server's configuration services and by the Redirector. The data is saved in the **NCoDServices.RAS.txt** file in the **private** directory (for example, C:\hostondemand\private).

Multiple Sessions



To create a multiple session icon you must set the:

Name

Type in the name you want your multiple session icon to have. It appears beneath the icon in the client window.

Start Sessions

The list of the names of the sessions to be started by this icon.

Sessions

The list of all the configured sessions available in the client window.

Related topics:

- [Multiple Session Icon Overview](#)

Multiple Session Icon Overview



A multiple session icon starts more than one previously configured session at a time. For example, you can create a multiple session icon that starts a 5250 emulator session and a 5250 host print session together. A multiple session icon can't start other multiple session icons. You can export and import multiple session icons, but the sessions that are started by the multiple session icon are not exported or imported along with it. Export or import those sessions separately.

To create a multiple session icon:

1. Open the Administration window.
2. Right click on a group or a user and select Sessions.
3. Click Multiple Sessions.

Note:

If no sessions have been previously configured you will see an error message stating that you must configure sessions before creating a multiple session icon.

4. Type a name for the multiple session icon in the multiple sessions window.
5. Select a session to add to the multiple session by clicking on a previously created session in the "Sessions" box to highlight the session, then click "Add". The name of the session will be added to the "Start Sessions" box. To remove a session from the multiple session, click on the session in the "Start Sessions" box to highlight it and then click "Remove".



If you delete or rename a session that is part of a multiple session, a message is displayed that the session is part of a multiple session icon and won't be started by the multiple session icon any longer. You can cancel the delete or rename action, or continue.

6. Click "OK" when you are finished.

The multiple session icon stores a list of the names of the sessions that it starts. If sessions in a multiple session have been configured with a session ID on the [Advanced](#) tab, the sessions are started in session ID order. If no session IDs are specified, the sessions will be started in the order they are added to the multiple session icon.

If a session can't be found (if it was renamed or deleted) it is not started, but Host On-Demand does not notify you that the session could not be found. If none of the sessions in the list can be found, Host On-Demand does display a message stating that none of the sessions exist.

Related topics:

- [Multiple Sessions](#)

Telnet-negotiated security overview

The Telnet-negotiated setting determines if the Transport Layer Security (TLS) negotiation between the client and the server is done on the established Telnet connection or on a TLS connection prior to Telnet negotiations. You can configure Telnet-negotiated security for Host On-Demand 3270 display and printer sessions. Telnet-negotiated security is an extension to Telnet that enables TLS to be negotiated over a Telnet connection. Telnet-negotiated security supports the [TLS Protocol Version 1.0](#). This protocol allows security negotiation from TLS 1.0 to SSL 3.0 for servers that do not support TLS 1.0.

You can [configure Telnet-negotiated security](#) in the session configuration properties on the server or on the client workstation. There is a Telnet-negotiated radio button that is not selectable until **Enable Security** is set to **Yes**. If **Enable Security** and **Telnet-negotiated** are both set to **Yes**, a TLS connection is negotiated after the normal Telnet connection is established. However, the 3270 session will not start until the TLS negotiation completes successfully. If the server does not support TLS-based Telnet Security, the session will not start, and an error message will be issued.

If **Enable Security** is set to **Yes** and **Telnet-negotiated** is set to **No**, TLS negotiations are done on a TLS connection with the server. The default setting is **No** because few Telnet servers support TLS-based Telnet Security. (IBM Communications Server version 2 release 10 is an example of a Telnet server that supports TLS-based Telnet Security.)

If **Enable Security** is set to **Yes** and **Telnet-negotiated** is set to **Yes**, then **Enable Security** is set back to **No** and **Telnet-negotiated** is no longer selectable. The session has *no* security, even though **Telnet-negotiated** is still set to **Yes** because Telnet-negotiated security requires **Enable Security** to be first set to **Yes**. To set **Telnet-negotiated** back to **No** you must first set **Enable Security** to **Yes** so that **Telnet-negotiated** is again selectable.

If **Enable Security** is set to **No** and the server requests a TLS-based Telnet Security session from the client, the Host On-Demand client cannot start a TLS-based Telnet Security session. An error message is then issued.

Related topic:

- [Telnet-negotiated security](#)
- [How TLS and SSL security work](#)
- [Configuring TLS and SSL](#)
- [TLS Protocol Version 1.0](#)

Using the Start PC Command (STRPCCMD) in Host On-Demand

Host On-Demand 5250 sessions support the Start PC Command (STRPCCMD). STRPCCMD allows you to launch an application on a personal computer that is attached to the host iSeries system. It is the only PC Organizer (PCO) function supported by Host On-Demand for 5250 sessions. STRPCCMD can be invoked directly from the AS/400 command line or through the Client Access/400 Organizer menu.

To use STRPCCMD, do the following:

1. Start a 5250 session.
2. Log into the iSeries host system.
3. Start PC Organizer. Enter the following command at the AS/400 command line:

```
STRPCO PCTA( *NO )
```

Host On-Demand does not support the PC Text Assist (PCTA) function of PC Organizer. You must specify a value of *NO for the PCTA parameter.

4. To run STRPCCMD, do one of the following:
 - From the Client Access/400 menu, select option 7 (Start a PC Command).
 - Enter the following at the AS/400 command line, then press the PF4 key:

```
STRPCCMD
```

5. Specify the full path name of the application (for example, C:\winnt\notepad.exe) at the PC Command prompt.

Note: You cannot directly execute MS-DOS commands (such as DIR, DATE, and TIME) with STRPCCMD. However, on the Windows 2000 and Windows NT platforms, you can use the cmd.exe application to run these commands. For example, to run the DIR command, specify the following at the PC Command prompt:

```
c:\winnt\system32\cmd.exe /c start DIR
```

6. Specify whether the computer should pause after running a command. Enter one of the following:

***YES**

The computer pauses after running the PC command, then returns to the iSeries session. If the PAUSE parameter is set to *YES, Host On-Demand waits for the PC process to complete and is blocked until the process exits. Host On-Demand waits for the parent process to complete even though the PC process executes a child process.

***NO**

The computer returns directly to the iSeries session.

Prompt



This window appears when you record and when you play a macro.

Recording

The window is asking you to type whatever information will allow the host application to continue. For example, if the application needs your user id, type it now and click OK. The text will not be entered on the screen when you play the macro, nor will it be saved in the macro. It's used as a placeholder to tell the macro that something must be typed at this point during playback. For example, if the application needs your user id, type it now and click OK. You cannot continue recording until you type the necessary information.

Playback

Type the appropriate information.

Resizing the Host On-Demand Window



You can resize your Host On-Demand session if it is a separate window.

To make the window wider, drag the window border to the size you want. Only horizontal resizing is currently supported.

If your session is a browser window, you cannot resize. You may have to scroll to view the entire window.

Viewing system properties

To view a client's system properties, click Actions > Problem Determination > System Properties. The client must be running the HODDebug.html applet to access this option. Values for the following items are displayed in the browser Java Console:

- Java program that is running
- Operating system installed
- User information
- File, path, and line separator statements (if AIX)

IBM Trademarks



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

AIX	CICS	DB2
IBM	OS/2	OS/400
RACF	VisualAge	VTAM

For a complete list of IBM trademarks, go to <http://www.ibm.com/legal/copytrade.phtml>.

Other trademarks

Lotus and WordPro are trademarks of Lotus Development Corporation in the United States, or other countries, or both.

Tivoli is a trademark of Tivoli Systems Inc. in the United States, or 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 and/or other countries.

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

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

Copyright Advanced Transition Technologies, Inc. 1996-1998

AT² and ResQ!Net are trademarks of Advanced Transition Technologies, Inc.

Netscape, Netscape Navigator, and Netscape Communicator are trademarks of Netscape Communications Corporation.

Epson ESC/P is a trademark of Epson Corporation.

HP PCL Level 3 is a trademark of Hewlett Packard Corporation.

Epson ESC/P is a trademark of Epson Corporation.

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

A

[accessibility](#)

[account, change a user's or a group's](#)

[account, creating your own user](#)

[accounts, enabling users to create](#)

[accounts, user](#)

[actions \(macro\)](#)

[adding buttons to toolbar](#)

[adding or modifying a user](#)

[adding sessions](#)

[adding a data extraction](#)

[adding a prompt to a macro](#)

[adding a smart wait \(macro\)](#)

[additional options, Deployment Wizard](#)

[adding or changing a group](#)

[additional parameters, Deployment Wizard](#)

[address, destination](#)

[administering statements \(database\)](#)

[administration client](#)

[administrator, logging on as an](#)

[administrator account](#)

[administrator user ID and password, changing](#)

[advanced options, Deployment Wizard](#)

[advanced options \(3270 print\)](#)

[Advanced tab \(FTP client\)](#)

[Advanced tab \(FTP client\), more](#)

[Advanced tab \(session configuration\)](#)

[aids, problem determination](#)

[AIX, running Certificate Management on agent support \(SLP\), directory appearance, disabling functions:](#)

[applet, Host On-Demand](#)

[Arabic language support](#)

[ASCII file types \(FTP client\)](#)

[assignment, key](#)

[associated printer session \(3270 display session\)](#)

[attributes, setting the display](#)

[authentication, client](#)

[authentication, obtaining certificates for client](#)

[authentication, using native](#)

[authentication, proxy server](#)

[authentication, server](#)

[auto-connect](#)

[auto-reconnect](#)

[auto-start](#)

[autostart configured sessions](#)

[autowrap](#)

[availability of the lpr client software](#)

B

[backspace](#)

[background colors, changing foreground or](#)

[basic configuration steps](#)

[bidirectional language support](#)

[binary options \(CICS\), receive](#)

[binary options \(CICS\), send](#)

[binary options \(MVS/TSO and VM/CMS\), receive](#)

[binary options \(MVS/TSO and VM/CMS\), send](#)

[binary options \(OS/400\), file transfer receive](#)

[binary options \(OS/400\), file transfer send](#)

[blink, cursor](#)

[bookmarks or icons, starting sessions with](#)

[browser troubleshooting](#)

[buttons, adding toolbar](#)

[buttons, editing toolbar](#)

C

[cache options, Deployment Wizard](#)

[cached client client help](#)

[cached client parameters, setting](#)

[cached clients, removing](#)

[caption settings, Database On-Demand](#)

[certificate, choose client](#)

[certificate, extracting a](#)

[certificate, obtaining for a server](#)

[certificate, obtaining for client authentication](#)

[certificate, server requesting](#)

[certificate, using a self-signed](#)

[certificate, viewing or saving a requesting server's](#)

[certificate from an unknown CA, using a server](#)

[certificate from a well-known \(trusted\) CA, using a server](#)

[certificate information, viewing or saving client](#)

[certificate information, viewing or saving issuer](#)

[certificate information, viewing server](#)

[Certificate Management on AIX, running](#)

[certificate password, changing](#)

[certificates available to clients, making](#)

[change a user's or a group's account](#)

[changing the administrator user ID and password](#)

[changing the current host session colors](#)

[changing a file transfer list](#)

[changing foreground or background colors](#)

[changing a group, adding or](#)

[changing a host defined to the Redirector](#)

[changing a macro](#)

[changing the Service Manager's configuration port](#)

[changing the trace settings \(client\)](#)

[character-cell size](#)

[character-cell size, selecting a](#)

[characters and functions, default](#)

[checking and upgrading the JVM level for Microsoft Internet Explorer](#)

[CICS gateway code page](#)

[CICS options \(file transfer\)](#)

[CICS, receive binary options](#)

[CICS, receive text options](#)

[CICS, send binary options](#)

[CICS, send text options](#)

[CICS server](#)

[clear before transfer](#)

[client, administration](#)

[client, Database On-Demand](#)

[client, download](#)

[client, Function On-Demand](#)

[client, new user](#)

[client, remove cached](#)

[client, tracing on the](#)

[client authentication](#)

[client certificate information, viewing or saving](#)

[client files, creating](#)

[client parameters, setting cached](#)

[client troubleshooting](#)

[client window](#)

[client window, disabling functions:](#)

[closing a session](#)

[CMS, receive file options \(MVS/TSO and VM/ \)](#)

[CMS, send file options \(MVS/TSO and VM/ \)](#)

[CMS options \(file transfer\), VM/](#)

[code page, host](#)

[codepage converter](#)

[color scheme, selecting a](#)

[colors, changing the current host session](#)

[colors, changing foreground or background](#)

[colors, remap graphics](#)

[colors, resetting the host session default](#)

[colors, understanding session](#)

[column heading settings, Database On-Demand](#)

[communications check \(comm check\)](#)

[compiling a printer definition file \(3270\)](#)

[conditional action \(macro\)](#)

[configuration model, Deployment Wizard](#)

[configure, selecting a session to](#)

[configuring the configuration servlet](#)

[configuring database options](#)

[configuring a host as a Redirector](#)

[configuring a host session for a user or group](#)

[configuring and managing Host On-Demand services](#)

[configuring an OS/400 proxy server](#)

[configuring a session](#)

[configuring a session to connect to the Redirector](#)

[configuring Host On-Demand with an IBM firewall](#)

[configuring SSL on clients](#)

[configuring Telnet-negotiated security](#)

[configuring TLS and SSL](#)

[confirm on exit](#)

[connecting a session](#)

[connection, disabling functions:](#)

[connection, setting up a new](#)

[Connection tab \(FTP client\)](#)

[Connection tab \(session configuration\)](#)

[considerations for selecting a report interval](#)

[copying a session](#)

[copying text](#)

[copying a user](#)

[create directory \(FTP client local file system\)](#)

[create directory \(FTP client remote file system\)](#)

[creating a desktop icon for a bookmarked session](#)

[creating an HTML file to bypass logon and start a configured session](#)

[creating an HTML file for starting sessions](#)

[creating a new host session](#)

[creating a statement](#)

[creating your own user account](#)

[cursor](#)

[cursor, blink](#)

[cursor style](#)

[Custom Function Editor](#)

[custom HTML templates, using](#)

[customize toolbar](#)

[customizing Client window icons](#)

[customizing hodptd.list and hodmodel.list](#)

[customizing a session using the Deployment Wizard](#)

[Cut/Copy tab](#)

[cutting text](#)

D

[data extraction, adding a](#)

[data extraction, adding to a macro](#)

[\(database\) statements](#)

[database, configuring options](#)

[database, file downloading](#)

[database, JDBC and other drivers](#)

[Database On-Demand](#)

[Database On-Demand caption settings](#)

[Database On-Demand client](#)

[Database On-Demand column heading](#)

[Database On-Demand File Upload](#)

[Database On-Demand, getting started with](#)

[Database On-Demand HTML table settings](#)

[Database On-Demand options for user, setting](#)

[Database On-Demand overview](#)

[Database On-Demand save results](#)

[Database On-Demand SQL statements](#)

[Database On-Demand table text settings](#)

[database tables](#)

[DBCS characters, displaying split](#)

[default, transfer mode](#)

[default colors, resetting the host session](#)

[default group, HOD](#)

[default keyboard mapping](#)

[default session configurations and user preferences](#)

[default shortcut keys](#)

[defaults, keyboard mapping](#)

[defaults, setting file transfer](#)

[delete, FTP client local file system](#)

[delete, FTP client remote file system](#)

[deleting a host from the Redirector](#)

[deleting a macro](#)

[deleting a session](#)

[deleting a statement](#)

[deleting a user or group](#)

[Deployment Wizard, additional parameters](#)

[Deployment Wizard, additional options](#)

[Deployment Wizard, advanced options](#)

[Deployment Wizard, cache options](#)

[Deployment Wizard, configuration model](#)

[Deployment Wizard, customizing HTML files](#)

[Deployment Wizard, deploying files using DWunzip](#)

[Deployment Wizard, disable functions](#)

[Deployment Wizard, edit existing HTML file](#)

[Deployment Wizard, file name and output format](#)

[Deployment Wizard, host sessions](#)

[Deployment Wizard, installing the](#)

[Deployment Wizard, logon type](#)

[Deployment Wizard, preload options](#)

[Deployment Wizard, troubleshooting](#)

[Deployment Wizard, server connection options](#)

[Deployment Wizard, starting](#)

[Deployment Wizard, welcome](#)

[description, macro](#)

[destination address](#)

[destination port](#)

[device status](#)

[directories, understanding](#)

[directory, migrating to an LDAP](#)

[directory, specifying the LDAP](#)

[directory agent support \(SLP\)](#)

[directory schema](#)

[Directory Utility, using the](#)

[disable functions, Deployment Wizard](#)

[disabling \(locking\) fields](#)

[disabling functions: appearance](#)

[disabling functions: client window](#)

[disabling functions: connection](#)

[disabling functions: file transfer](#)

[disabling functions: macro](#)

[disabling functions: other](#)

[disabling functions: preferences](#)

[disabling functions: printer](#)

[disabling functions through HTML files](#)

[disabling graphical interface functions](#)

[disconnecting a session](#)

[display attributes, setting the](#)
[distinguished name, required for LDAP](#)
[DOS to a PPA printer \(HP Desk Jet 700 series\), printing from](#)
[download client](#)
[download file, database](#)
[drivers, JDBC, using others, database](#)
[DWunzip, using to deploy Deployment Wizard files](#)
[dynamic query](#)
[dynamically modifying session properties \(HTML overrides\)](#)

E

[echo, local](#)
[edit existing HTML file, Deployment Wizard](#)
[editing a macro](#)
[editing macro links](#)
[editing macro screen definitions](#)
[EHLLAPI enablement tool](#)
[emulation limitations, VT 420](#)
[enable security](#)
[enable SLP](#)
[enabling host graphics](#)
[enabling license usage counting](#)
[enabling users to create accounts](#)
[error codes, OIA](#)
[error messages](#)
[exercise, Macro Manager](#)
[exit, confirm on](#)
[export sessions](#)
[export session, overwrite existing file?](#)

[express logon feature](#)

[express logon macro, recording](#)

[external commands after host print jobs, running](#)

[extracting a certificate](#)

F

[field, blink](#)

[field lock, numeric](#)

[file, download, database](#)

[file, viewing a trace of a user](#)

[file name and output format, Deployment Wizard](#)

[file path and name](#)

[file transfer, CICS options](#)

[file transfer, defaults](#)

[file transfer default options, setting](#)

[file transfer list, changing a](#)

[file transfer on host](#)

[file transfer overview](#)

[file transfer using FTP](#)

[file transfer, clear before transfer](#)

[file transfer, disabling functions:](#)

[file transfer, general options](#)

[file transfer, MVS/TSO options](#)

[file transfer, OS/400 options](#)

[file transfer, receive binary options \(CICS\)](#)

[file transfer, receive binary options \(MVS/TSO and VM/CMS\)](#)

[file transfer, receive binary options \(OS/400\)](#)

[file transfer, receive text options \(CICS\)](#)

[file transfer, receive text options \(MVS/TSO and VM/CMS\)](#)

[file transfer, receive text options \(OS/400\)](#)

[file transfer, send binary options \(CICS\)](#)

[file transfer, send binary options \(MVS/TSO and VM/CMS\)](#)

[file transfer, send binary options \(OS/400\)](#)

[file transfer, send text options \(CICS\)](#)

[file transfer, send text options \(MVS/TSO and VM/CMS\)](#)

[file transfer, send text options \(OS/400\)](#)

[file transfer, VM/CMS options](#)

[file types, ASCII](#)

[File Upload, Database On-Demand](#)

[files \(FTP client local file system\), send](#)

[files \(FTP client remote file system\), receive](#)

[files using Host File Transfer, transferring](#)

[firewall, configuring Host On-Demand with an IBM](#)

[firewall, using the configuration servlet through the](#)

[font](#)

[font name](#)

[font style](#)

[foreground or background colors, changing](#)

[FTP client, Advanced tab](#)

[FTP client, Connection tab](#)

[FTP client, More Advanced tab](#)

[FTP client, quote command](#)

[FTP client, Screen tab](#)

[FTP client, transfer list manager](#)

[FTP client local file system, create directory](#)

[FTP client local file system, delete](#)

[FTP client local file system, rename](#)

[FTP client local file system, send files](#)

[FTP client local file system, send files as](#)

[FTP client overview](#)

[FTP client remote file system, create directory](#)

[FTP client remote file system, delete](#)

[FTP client remote file system, receive files](#)

[FTP client remote file system, receive files as](#)

[FTP client file system, rename](#)

[FTP client session window](#)

[FTP file transfer](#)

[function comparison, host graphics](#)

[function keys](#)

[Function On-Demand client](#)

[functions, disabling](#)

G

[general, macro](#)

[general help information](#)

[general options, file transfer](#)

[getting started with Database On-Demand](#)

[graphical user interface, Screen Customizer](#)

[graphics, enabling host](#)

[graphics, remap colors](#)

[graphics function comparison, host](#)

[graphics-order list](#)

[group, adding or changing a](#)

[group, configuring a host session for a user or](#)

[group, deleting a user or](#)

[group IDs, valid](#)

[group membership](#)

[group's account, change a user's or a](#)

[GUI, Screen Customizer](#)

H

[Hebrew language support](#)

[help, before calling IBM](#)

[help, message](#)

[help, sources of](#)

[help information, general](#)

[Hindi enablement, understanding](#)

[history, viewing status bar](#)

[hodpdt.list and hodmodel.list, customizing](#)

[host code page](#)

[host directory listing](#)

[host file transfer](#)

[host functions, assigning keys to](#)

[host graphics](#)

[host graphics, enabling](#)

[host graphics function comparison](#)

[Host On-Demand predefined clients](#)

[Host On-Demand Redirector, using the](#)

[Host On-Demand server configuration from one server to another, moving your](#)

[Host On-Demand services](#)

[Host On-Demand Service Manager](#)

[Host On-Demand with an IBM firewall, configuring](#)

[Host On-Demand 2.0 group](#)

[host session, creating a new](#)

[host session colors, changing the current](#)

[host session default colors, resetting the](#)

[host to a workstation \(3270\), printing directly from a](#)

[host to a workstation \(5250\), printing directly from a](#)

[Host Printing Reference](#)

[host print jobs, running external commands after](#)

[host sessions](#)

[host sessions, Deployment Wizard](#)

[HTML client files, creating](#)

[HTML file for starting sessions, creating an](#)

[HTML file to bypass logon and start a configured session, creating an](#)

[HTML files, disabling functions through](#)

[HTML files, setting up a separate user publish directory for](#)

[HTML table settings, Database On-Demand](#)

[HTML templates, custom](#)

[HTTP proxy server](#)

I

[icons, customizing Client window](#)

[icons, creating for a bookmarked session](#)

[ID/password, administrator](#)

[information area, operator](#)

[information, general help](#)

[importing sessions](#)

[importing Personal Communications 3270 printer sessions](#)

[Information Bundler](#)

[installing the Deployment Wizard](#)

[Internet Explorer, checking and upgrading the JVM level for Microsoft](#)

[IPMonitor](#)

[IPMonitor v1.0 automatic mode, configuring](#)

[IPMonitor v1.0 for Java](#)

[IPMonitor v1.0 for Java, automatic mode](#)

[IPMonitor v1.0 for Java, normal mode](#)

[IPMonitor v1.0 for Java application, configuring](#)

[IPMonitor v1.0 for Java application, starting](#)

[IPMonitor v1.0 for Java normal mode, starting](#)

[iSeries name \(SLP\)](#)

[iSeries troubleshooting](#)

J

[Java troubleshooting](#)

[JDBC drivers, registering \(database\)](#)

[JDBC drivers, using others \(database\)](#)

[join, remove](#)

[join, table alias](#)

[join, table fields](#)

[join, types](#)

[jump to next session](#)

[JVM level for Microsoft Internet Explorer, checking and upgrading](#)

K

[key assignment](#)

[key repetition](#)

[keyboard, remapping the](#)

[keyboard, unlocking the](#)

[keyboard, using to draw and move the trim box](#)

[keyboard mapping, default](#)

[keypad](#)

[keypad, showing](#)

[keys, default shortcut](#)

[keys, specifying as repeating or non-repeating](#)

L

[language support, bidirectional](#)

[language support, national](#)

[language support, thai](#)

[language support, understanding VT bidirectional](#)

[Language tab, session configuration](#)

[LDAP, implications of migrating to](#)

[LDAP, migrating to](#)

[LDAP, setting up and using](#)

[LDAP, specifying directory information](#)

[LDAP, understanding](#)

[LDAP directory schema](#)

[levels, setting trace](#)

[license usage](#)

[license usage, enabling counting](#)

[license usage, viewing](#)

[light pen, using](#)

[limitations, security](#)

[list, changing a file transfer](#)

[list, deleting](#)

[list, editing](#)

[local echo](#)

[locked keyboard](#)

[logging on as an administrator](#)

[logging on as a user](#)

[logon window, bypassing the](#)

[logon feature, express](#)

[Logon tab](#)

[logon type, Deployment Wizard](#)

[log and trace messages, format](#)

[log file, viewing](#)

[logs, viewing the user](#)

[lpr client software, availability of the](#)

[LU name](#)

M

[macro, actions](#)

[macro, adding a prompt](#)

[macro, adding a prompt to a](#)

[macro, adding a smart wait](#)

[macro, adding as toolbar button](#)

[macro, assigning keys to](#)

[macro, changing](#)

[macro, conditional action](#)

[macro, deleting](#)

[macro, description](#)

[macro, disabling functions:](#)

[macro, editing](#)

[macro, editing screen definitions](#)

[macro, exporting](#)

[macro, express logon](#)

[macro, general](#)

[macro, importing](#)

[macro, playing](#)

[macro, recording](#)

[macro, recording an express logon](#)

[macro, using variables and arithmetic expressions](#)

[macro editor, using the](#)

[macro links, editing](#)

[Macro Manager exercise](#)

[Macro Manager, showing](#)

[Macro Manager, using the](#)

[macro variables](#)

[making certificates available to clients](#)

[managing and configuring Host On-Demand services](#)

[managing users and groups](#)

[mapping, default keyboard](#)

[marking text](#)

[maximum wait time \(SLP\)](#)

[membership, group](#)

[menu commands, assigning keys to](#)

[message and trace log, viewing the server's](#)

[messages format, log and trace](#)

[messages, error](#)

[Microsoft Internet Explorer, checking and upgrading the JVM level for](#)

[migrating to LDAP, implications of](#)

[migrating to an LDAP directory](#)

[modifying a session configuration](#)

[modifying a session configuration, administrator](#)

[modifying a user, adding or](#)

[modifying session properties \(HTML overrides\), dynamically](#)

[More Advanced tab \(FTP client\)](#)

[moving your Host On-Demand server configuration from one server to another](#)

[multiple sessions](#)

[multiple session icon overview](#)

[MVS/TSO options](#)

[MVS/TSO and VM/CMS, receive binary options](#)

[MVS/TSO and VM/CMS, receive text options](#)

[MVS/TSO and VM/CMS, send binary options](#)

[MVS/TSO and VM/CMS, send text options](#)

N

[national language support](#)

[native authentication, using](#)

[Native Windows Print](#)

[network tuning \(SLP\)](#)

[new-line operation](#)

[new user client](#)

[numeral shape](#)

[numeric field lock](#)

O

[obtaining certificates for client authentication](#)

[obtaining a server certificate](#)

[OIA, showing](#)

[OIA \(Operator Information Area\)](#)

[opening a statement](#)

[options, configuring \(database\)](#)

[options, setting the default file transfer](#)

[Options tab, database](#)

[OS/400, receive binary options](#)

[OS/400, receive text options](#)

[OS/400, send binary options](#)

[OS/400, send text options](#)

[OS/400 options, file transfer](#)

[OS/400 proxy server](#)

[OS/400 proxy server, configuring](#)

[other, disabling functions:](#)

[overview, Database On-Demand](#)

[overview, file transfer](#)

[overview, FTP client](#)

[overview, multiple session icon](#)

[overview, Telnet-negotiated security overview](#)

[overwrite existing file? \(export session\)](#)

P

[PA1](#)

[PA2](#)

[parameters, session](#)

[parameters, setting cached client](#)

[password, changing the administrator user ID and](#)

[Paste tab](#)

[pasting text](#)

[PC code page options](#)

[PC Command \(STRPCCMD\), Start](#)

[PDF \(printer definition files\)](#)

[PDT \(printer definition tables\)](#)

[PDT compiler](#)

[Personal Communications 3270 printer sessions, importing](#)

[playing a macro](#)

[pool name](#)

[port, changing the Service Manager's configuration](#)

[portlet, deploying Host On-Demand as a](#)

[preferences, user](#)

[preload options, Deployment Wizard](#)

[Print, Native Windows](#)

[print buffer size](#)

[print destination](#)

[print job status](#)

[print jobs, formatting pages](#)

[print jobs, setting up](#)

[print jobs, running external commands after host](#)

[printer name](#)

[printer options, advanced](#)

[printer sessions, importing Personal Communications 3270](#)

[printer status](#)

[Printer tab, session configuration](#)

[printing directly from a host to a workstation \(3270\)](#)

[printing directly from a host to a workstation \(5250\)](#)

[printing from DOS to a PPA printer \(HP Desk Jet 700 series\)](#)

[printing a screen](#)

[printing troubleshooting](#)

[problem determination aids](#)

[problems, browser](#)

[problems, client](#)

[problems, Deployment Wizard](#)

[problems, iSeries](#)

[problems, Java](#)

[problems, known \(troubleshooting\)](#)

[problems, miscellaneous](#)

[problems, printing](#)

[problems, Redirector](#)

[problems, security](#)

[problems, zSeries](#)

[program check \(prog check\)](#)

[prompt \(macro\)](#)

[prompt, adding to a macro](#)

[properties, viewing system](#)

[Proxy Server tab](#)

[proxy server, configuring an OS/400](#)

[proxy server, OS/400](#)

[publishing, Web page \(database\)](#)

Q

[query, dynamic](#)

[quote command, FTP client](#)

R

[receive binary options \(CICS\)](#)

[receive binary options \(MVS/TSO and VM/CMS\)](#)

[receive binary options \(OS/400\)](#)

[receive files \(FTP client remote file system\)](#)

[receive text options \(CICS\)](#)

[receive text options \(MVS/TSO and VM/CMS\)](#)

[receive text options \(OS/400\)](#)

[recording an express logon macro](#)

[recording a macro](#)

[register JDBC drivers, database](#)

[remapping the keyboard](#)

[Redirector, changing a host defined to the](#)

[Redirector, configuring a host as a](#)

[Redirector, configuring a session to connect to the](#)

[Redirector, deleting a host from the](#)

[Redirector, setting up with SSL](#)

[Redirector, using the Host On-Demand](#)

[Redirector, troubleshooting](#)

[remap_graphics colors](#)

[removing cached clients](#)

[rename \(FTP client local file system\)](#)

[rename \(FTP client remote file system\)](#)

[repeating, specifying a key as repeating or non-repeating](#)

[repetition, key](#)

[resetting the host session default colors](#)

[resizing the Host On-Demand window session](#)

[running Certificate Management on AIX](#)

[running external commands after host print jobs](#)

[running a statement](#)

S

[save results, database](#)

[schema, directory, LDAP](#)

[schema, installing extensions for LDAP](#)

[scope, SLP](#)

[screen, printing a](#)

[Screen Customizer/LE for Host On-Demand](#)

[screen definitions, editing macro](#)

[screen size](#)

[Screen tab, FTP client](#)

[Screen tab \(session configuration\)](#)

[security, changing the administrator user ID and password](#)

[security, changing certificate settings](#)

[security, choose certificate](#)

[security, client authentication](#)

[security, configuring SSL on clients](#)

[security, configuring Telnet-negotiated security](#)

[security, configuring TLS and SSL](#)

[security, database](#)

[security, enable](#)

[security, express logon feature](#)

[security, extracting a certificate](#)

[security, making server certificates available to clients](#)

[security, obtaining certificates for client authentication](#)

[security, obtaining a server certificate](#)

[security, troubleshooting](#)

[security, running Certificate Management on AIX](#)

[security, server requesting certificate](#)

[security, Telnet-negotiated security overview](#)

[security, using native authentication](#)

[security, using a self-signed certificate](#)

[security, viewing or saving client certificate information](#)

[security, viewing or saving issuer certificate information](#)

[security, viewing or saving a requesting server's certificate](#)

[security, viewing server certificate information](#)

[security limitations](#)

[Security tab \(session configuration\)](#)

[selecting a character-cell size](#)

[selecting a color scheme](#)

[selecting a session to configure](#)

[send binary options \(CICS\)](#)

[send binary options \(MVS/TSO and VM/CMS\)](#)

[send binary options \(OS/400\)](#)

[send files \(FTP client local file system\)](#)

[send text options \(CICS\)](#)

[send text options \(MVS/TSO and VM/CMS\)](#)

[send text options \(OS/400\)](#)

[separate files](#)

[server, basic steps to configure](#)

[server, tracing on the](#)

[server authentication](#)

[server authentication, enabling](#)

[server certificate from an unknown CA, using a](#)

[server certificate from a well-known \(trusted\) CA, using a](#)

[server certificate information, viewing](#)

[server configuration from one server to another, moving your Host On-Demand](#)

[server connection options, Deployment Wizard](#)

[server support and limitations, SLP](#)

[server's message and trace log, viewing the](#)

[service location protocol \(SLP\)](#)

[Service Manager, Host On-Demand](#)

[Service Manager's configuration port, changing the](#)

[services, Host On-Demand](#)

[servlet, configuring the configuration servlet](#)

[session, creating a new host](#)

[session, new](#)

[session, multiple session icon overview](#)

[session, printer](#)

[Session 1 and Session 2, using](#)
[session colors, changing the current host](#)
[session colors, understanding](#)
[session configurations, storing](#)
[session name](#)
[session parameters](#)
[session properties \(HTML overrides\), dynamically modifying](#)
[session status](#)
[session window, resizing the Host On-Demand](#)
[sessions, adding](#)
[sessions, automatically starting](#)
[sessions, configuring](#)
[sessions, connecting](#)
[sessions, copying](#)
[sessions, ending](#)
[sessions, exporting](#)
[sessions, importing](#)
[sessions, importing Personal Communications 3270 printer](#)
[sessions, jump to next](#)
[sessions, multiple](#)
[sessions, starting with bookmarks or icons](#)
[sessions area, active](#)
[sessions for a user or a group, configuring host](#)
[setting cached client parameters](#)
[setting Database On-Demand options for users](#)
[setting the display attributes](#)
[setting trace levels](#)
[setting up a new connection](#)
[setting up and using LDAP](#)

[settings, changing the \(client\) trace](#)

[settings, Database On-Demand caption](#)

[settings, Database On-Demand column heading](#)

[settings, Database On-Demand HTML table](#)

[settings, table text](#)

[shared user accounts](#)

[shortcut keys, default](#)

[show toolbar](#)

[show toolbar text](#)

[SLP \(Service Location Protocol\)](#)

[SLP, iSeries name](#)

[SLP, directory agent support](#)

[SLP administration](#)

[SLP limitations](#)

[SLP requirements to run on a token ring](#)

[smart wait, adding to a macro](#)

[Socks proxy server](#)

[sort, database](#)

[specifying a key as repeating or non-repeating](#)

[specifying the LDAP directory information](#)

[split DBCS character](#)

[SQL statements, Database On-Demand](#)

[SSL \(Secure Socks Layer\) protocol](#)

[SSL, setting up Redirector using](#)

[start Host On-Demand services](#)

[Start PC command \(STRPCCMD\)](#)

[starting another identical session](#)

[starting the Deployment Wizard](#)

[starting a session](#)

[statement, copying](#)

[statement, creating](#)

[statement, deleting](#)

[statement, opening](#)

[statement, renaming](#)

[statement, running](#)

[statement, types](#)

[statements, database](#)

[status, device](#)

[status, print job](#)

[status bar history, viewing](#)

[storing user preferences](#)

[suffix, required for LDAP](#)

[support, national language](#)

[switching to another session](#)

[system properties, viewing](#)

T

[tab, Advanced \(session configuration\)](#)

[tab, Connection \(session configuration\)](#)

[tab, Cut/Copy](#)

[tab, Language \(session configuration\)](#)

[tab, Paste](#)

[tab, Printer \(session configuration\)](#)

[tab, Screen \(session configuration\)](#)

[tab, Security \(session configuration\)](#)

[tab, Trim](#)

[tab, VT Display \(session configuration\)](#)

[table text, Database On-Demand](#)

[table text settings](#)

[tables, customizing \(database\)](#)

[tables, database](#)

[tables, join \(database\)](#)

[Telnet-negotiated security, configuring](#)

[Telnet-negotiated security, overview](#)

[terminal type](#)

[text, copying](#)

[text, cutting](#)

[text, marking and unmarking](#)

[text, pasting](#)

[text options \(CICS\), receive](#)

[text options \(MVS/TSO and VM/CMS\), receive](#)

[text options \(OS/400\), receive](#)

[text options \(CICS\), send](#)

[text options \(MVS/TSO and VM/CMS\), send](#)

[text options \(OS/400\), send](#)

[text orientation \(Arabic/Hebrew only\)](#)

[text type \(Arabic/Hebrew only\)](#)

[Thai language support](#)

[this scope only \(SLP\)](#)

[timeout options](#)

[TLS \(Transport Layer Security\) protocol](#)

[TLS-based Telnet Security](#)

[TN3270E](#)

[toolbar, customize](#)

[toolbar, show](#)

[trace, starting and stopping for a service](#)

[trace, viewing of a user's session](#)

[trace levels, setting](#)

[trace settings, changing the \(client\)](#)

[TraceOptions HTML parameter](#)

[TraceOptions HTML parameter, configuring](#)

[tracing on the client](#)

[tracing on the server](#)

[trademarks](#)

[transfer list, changing a file](#)

[transfer list manager, FTP client](#)

[transferring files using FTP](#)

[transferring files using Host File Transfer](#)

[Trim tab](#)

[troubleshooting](#)

[TSO, receive binary options \(VM/CMS and MVS/](#)

[TSO, receive text options \(VM/CMS and MVS/](#)

[TSO, send binary options \(VM/CMS and MVS/](#)

[TSO, send text options \(VM/CMS and MVS/](#)

[TSO options \(file transfer\), MVS/](#)

[tuning the network, SLP](#)

U

[understanding directories](#)

[understanding Hindi enablement](#)

[understanding session colors](#)

[understanding the OIA](#)

[understanding VT bidirectional support](#)

[unlocking the keyboard](#)

[unmarking text](#)

[upgrading the JVM level for Microsoft Internet Explorer, checking and](#)

[upgrading Host On-Demand](#)

[Upload, Database On-Demand File](#)

[user, copying a](#)

[user \(Host On-Demand\), logging on as a](#)

[user account, creating your own](#)

[user IDs, valid](#)

[user or group, configuring host sessions for](#)

[user or group, deleting a](#)

[user preferences](#)

[user preferences, storing](#)

[user prompt, adding to a macro](#)

[users, adding or modifying a](#)

[users, configuring host sessions for](#)

[users and groups, managing](#)

[users to create accounts, enabling](#)

[user's or a group's account, change a](#)

[user's session, viewing a trace of a](#)

[using custom HTML templates](#)

[using the Directory Utility](#)

[using the keyboard to draw and move the trim box](#)

[using LDAP, setting up and](#)

[using a light pen](#)

[using the Macro Editor](#)

[using the Macro Manager](#)

[using a self-signed certificate](#)

[using a server certificate from an unknown CA](#)

[using a server certificate from a well-known \(trusted\) CA](#)

[using variables and arithmetic expressions \(macro\)](#)

V

[valid group IDs](#)

[valid user IDs](#)

[variables, macro](#)

[viewing logs](#)

[viewing or saving a requesting server's certificate information](#)

[viewing or saving client certificate information](#)

[viewing or saving issuer certificate information](#)

[viewing server certificate information](#)

[viewing the server's message and trace logs](#)

[viewing status bar history](#)

[viewing system properties](#)

[viewing a trace of a user's session](#)

[VM/CMS, receive binary options \(MVS/TSO and\)](#)

[VM/CMS, receive text options \(MVS/TSO and\)](#)

[VM/CMS, send binary options \(MVS/TSO and\)](#)

[VM/CMS, send text options \(MVS/TSO and\)](#)

[VM/CMS options \(file transfer\)](#)

[VT 420 emulation limitations](#)

[VT bidirectional language support, understanding](#)

[VT Display tab \(session configuration\)](#)

W

[wait time \(SLP\)](#)

[Web page publishing](#)

[window, client](#)

[window, resizing the Host On-Demand session](#)

[Wizard, Deployment](#)

[workstation \(3270\), printing directly from a host to a](#)

[workstation \(5250\), printing directly from a host to a](#)

[workstation ID](#)

Z

[zSeries troubleshooting](#)