IBM® Host On-Demand

Welcome to IBM Host On-Demand Version 5.0 Help

Click any help topic in the Table of Contents to the left.

Click **Basic Steps for Getting Started** for basic steps to configuring and starting Host On-Demand.

Click  in the top right hand corner of any help topic to return to return to this overview.

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

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.

Basic configuration steps

After installing a Host On-Demand Server, you'll need to make some decisions about what functions to use. It's helpful to make these decisions before starting the Administration window so that you can have the information necessary to configure those functions.

The readme contains late-breaking product information.

Conceptual overviews

- Database On-Demand

  Refer to the Getting Started for:

- SSL security
- Redirector
- License use count or license use management
- Download clients, locally installed clients, or both
- Shared accounts, individual accounts, or both.

Once you have decided what functions of Host On-Demand to use, configure the server and clients. Each section provides basic configuration steps to get you started. Use the online help for detailed steps on completing the task.

- Configuring the server
  - Host On-Demand
  - Database On-Demand

- Configuring locally installed clients
  - Host access
  - Database On-Demand

Configuring the server for Host On-Demand

These steps assume you have already installed the Host On-Demand Server. Use the online help for detailed steps on completing these tasks.
Steps 4, 5, and 6 do not apply if you have only locally installed clients.

1. **Open the Administration window**.
   On Windows NT, click Start > Programs > IBM Host On-Demand > Administration > Administration Utility (or click the link above). On other platforms, load http://*server_name*/HOD/HODAdmin.html in your browser. You can open the Administration 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 password**.
   Click Users/Groups. Click HOD (System Default Group). Right click admin in the list of users and select properties. For security reasons, you should probably change the default administrator password. Type in a new password in the New Password field and again in the change password field. Click OK for the change to take effect.

4. **Add groups**.
   Click New Group to add a group. A group consists of one or more users. Host sessions can be defined for groups and users can be made members of one or more groups, reducing configuration and administration.
   Detailed steps

5. **Add users**.
   Click New User to add a new user. Each user must have an ID to log on to Host On-Demand.
   Detailed steps

6. **Configure host sessions for users and groups**.
   Right click on a user or group and select Sessions. Select a session type. Sessions defined to a group are available to all the users in that group.
   Detailed steps

7. **Enable security**.
   To use SSL for a session, open the properties for a session, click the Security tab and then click Enable Security. Use the Certificate Wizard or Certificate Management to request a server certificate or import an existing certificate that clients will need.
   Detailed steps

8. **Tell users how to start the download clients**.
   There are several ways that users can start the download clients:
   - Start page, HODMain.html
   - Client file name (for example, http://*hod_server_name*/hod/hod.html)
   - Customized HTML page

9. If you are using SSL client authentication, send a client certificate file and password to each user.

Configuring the server for Database On-Demand

The Database On-Demand client lets you extract data from an AS/400 database for use in a workstation application. Use the online help for detailed steps on completing these tasks.

1. **Open the Administration window.**
   On Windows NT, click Start > Programs > IBM Host On-Demand > Administration > Administration Utility. On other platforms, load the HODAdmin.html file into a browser. You can open the Administrator window from any computer that has access to the Host On-Demand server. The default user ID is *admin* and the password is *password*.

2. **Change your password**.
   Click the Users tab. Select admin from the User List and click Change. For security reasons, you should probably change the administrator password.

3. **Add groups (if needed)**.
   Click New Group to add a group. A group consists of one or more users. Statements and settings can be defined for groups and users can be made members of one or more groups, reducing configuration and administration.
   Detailed steps

4. **Add users (if needed)**.
   Click New User to add a new user. Each user must have an ID to log on to Host On-Demand.
   Detailed steps

5. **Define database options**.
   Right click the group or user and select Database > options to define database options for each user and group.
   Detailed steps

6. **Define SQL statements for each user**.
   Load the database client, HODDatabase.html, into a browser. Log on as the user that you are defining statements for. Define the SQL statements, save them, and then log off. Once statements are defined, you can copy them to other users or groups from the Administration window.
   Detailed steps

7. **Give users access to the database client**.
   There are several ways you can give users access:
   - Start page HODMain.html
   - Client name, HODDatabase.html
   - Customized HTML page

Configuring locally installed clients for host access

These steps assume you have already installed the Host On-Demand local client. A locally installed client is installed on a workstation and not downloaded from the server. Use the online help for detailed steps on completing these tasks.

1. **Start the Host On-Demand client**.
   Click Start > Programs > IBM Host On-Demand > Host On-Demand.

2. **Add sessions**.
   1. Click Default Sessions.
   2. Right click the session you want to configure and click Copy.

3. **Configure your session**.
   If you are connecting to a host through the Redirector, enter the host name or IP address of the Host On-Demand server on which the Redirector is running. 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.

4. **Enable security**
   Click the Security tab. To use SSL for this session, click Enable security.

Configuring locally installed clients to use Database On-Demand

The Database On-Demand client lets you extract data from an AS/400 database for use in a workstation application. Use the online help for detailed steps on completing the task.

1. **Start the database client**.
   Click Start > Programs > IBM Host On-Demand > Host On-Demand.

2. To change database options, click Options.

3. To define SQL statements, click New.

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 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)

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 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 5.0 format and added to their 5.0 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 5.0, it is `hostondemand`. If you have installed 5.0 in the original (3.0) root directory, you need do nothing more. However, if you have installed 5.0 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. These

preferences (the attributes that are different from the definitions that the administrator made) are saved in their accounts and do not affect the sessions of other users. The next time they start the same session, their preferences will be active. If changes are made to 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. 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.

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:

- Preferences saved by one user do not apply to any other user and cannot be copied or transferred to any other user. For example, if user A creates a macro, only A can use it.
- 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.
- Every preference and macro saved in a user's account is downloaded when the user logs on. If the user customizes a given field, then none of the changes made by the administrator to that field is inherited. However, you can export a session and distribute it to other users, who can import it. In this case, all the session's attributes are imported too.

Related topics

- Creating your own user account

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.

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). Group IDs are always 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.

Enabling users to create accounts

If you select **Allow users to create accounts** 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.

   LDAP 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.
<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.
<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.

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.

Adding or modifying a user

To allow users to create accounts for themselves or for other users, 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). User IDs are always 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.

   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.

   LDAP 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.

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. The user is added to the list of members for that group.

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**.

   LDAP 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.

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

Disabling graphical interface functions

To enable or disable functions for a group or user:

1. Click Users/Groups on the Administration window.
2. Right-click a group or user and select Disable Function.

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 menu 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.

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 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.

Functions can be disabled when configuring a user or group in the Administration 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.

Functions can also be disabled when creating a client HTML file using the Deployment Wizard.

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

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's 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. If at least one those groups has the function enabled, then the function is enabled for the user.

Disabling functions using the Deployment Wizard

If you are using the Deployment Wizard to create client HTML files, you can disable or enable

functions. Session configuration is loaded from the HTML file and not the Host On-Demand configuration server. Using the wizard, you can determine what functions should be enabled or disabled.

Related topics

- Starting the Deployment Wizard

Using 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 OS/390) 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.

Requirements for using native platform authentication include:

- Native platform authentication service must be installed on a Windows NT, AIX, or OS/390 Host On-Demand server. On Windows NT, native platform authentication requires Windows NT Server or Windows Advanced NT Server (Lanman) with a non-null domain.
- On the Host On-Demand server, LDAP must be enabled and users must have Native Authentication enabled.
- On Windows NT, the native user IDs must be enabled to allow batch logon.

To use native platform authentication on Host On-Demand:

1. Install native platform authentication service.
2. Start the native platform authentication service.
3. Configure current users for native authentication.
4. Enable Windows NT users for native authentication.

Installing native platform authentication

The files to support native platform authentication are installed with the Host On-Demand server. On Windows NT, the following additional steps are required:

1. Using regedit, find the registry value for:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK\CurrentVersion\BinPath
   ```

   For example: c:\ProgramFiles\IBM\GSK\bin. Add the value to the Path system variable. System variables can be edited using the Environment tab of the System icon in the Control Panel.

2. Define the environment variable **hod_dir** and set the value to the drive letter where Host On-Demand is installed (hod_dir=c:).

3. Using Windows NT Explorer, locate the file odsrapd.reg in the Host On-Demand bin directory. Add the registry settings defined in the file by double-clicking on the file.

4. Using regedit, find the registry value for:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\IBM\On-Demand Server for Windows NT\2.0\ir
   ```

   Edit the installpath value so that "%hod_dir%" is replaced with the drive letter where Host On-Demand is installed. For example, if Host On-Demand is installed on the d drive, change:

```
%hod_dir%\hostondemand\private
```

to

```
d:\hostondemand\private
```

5. Reboot your system.

Starting native platform authentication service

To start native platform authentication service:

Windows NT

The native platform authentication service is started from the Windows NT Services menu. By default, this service is set to start automatically.

AIX and OS/390

On the computer where the native platform authentication service (ODSRAPD) is installed, enter the following command:

```
odsrapd.sh [parameters]
```

Parameters

-l

Enables logging. You can also specify **-L**, **/l**, or **/L**

-t*xx*

Sets the socket timeout to some other value instead of the default 20 seconds. You can also specify **-T**, **/t**, or **/T** . *xx* is the new timeout value.

-c*xx*

Specifies the number of requests the server will allow. You can also specify **-C**, **/c**, or **/C**. *xx* is the new number of requests the server will handle.

Configuring current users for native authentication

Users' identities are verified as part of the log in process before they access host applications. For each user, select to use native authentication for identity verification.

To use native platform for authentication, you must first install the platform authentication service on the system used to authenticate users. The user's ID and password should already be defined to the operating system running the platform authentication service.


To use native platform authentication on Windows NT, you must grant the users an additional privilege before they can be authenticated.

To choose native platform authentication for a user:

1. Right-click a user and select Properties.
2. Check Use Native Authentication so that it is enabled.
3. Enter the user's ID for the native platform.
4. Click OK to close the window.

When a user logs on, the user ID and password are sent to the Host On-Demand service manager. The service manager sends a request for logon information about the user to the LDAP server. The LDAP server returns the requested user information and whether or not the user is configured for native authentication. 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.

Enabling Windows NT users for native platform authentication

1. Open the User Manager on Windows NT. This is normally found under: Start > Programs > Administrative Tools (Common) > User Manager.
2. Click Policies > User Rights from the menu bar of the User Manager.
3. Check Show Advanced User Rights.
4. In the Right field, select **Log on as a batch job**.
5. Click Add.
6. Select, from the Names field, users who will be using native platform authentication and click Add. To add members of a group, select the group and click Members. As you add users, the users' names are displayed in the Add Names field.
7. When you are finished adding users, click OK to close the Add Users and Groups window and save your changes.
8. Click OK to close the User Rights Policy dialog.
9. You can now exit the User Manager. All users that were granted the **Log on as a batch job** right can be authenticated using the native platform authentication service.

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. Users can also create and configure sessions.

Creating a session

1. Click Start > IBM Host On-Demand > Administration > Administration Utility.
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.

Adding a session configuration

1. Click Add Sessions on the Client window.
2. Right-click the type of session you want to add.
3. Click Copy.
4. Type or select the required information.
   Note: If a field is unavailable (shaded), it has been locked by a selection you made for another field or your administrator has chosen to not allow changes to that field.
5. Click OK.
6. Click Close to close the Add Sessions window. An icon is added to the Configured sessions window.

The Add Sessions window contains those sessions configured for the groups of which the user is a member.

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.

Related topics

- Copying a session
- Configuring a session for easy launch
- Deleting a session

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.

Creating an HTML file for starting sessions

You can create your own HTML files and provide them to users instead of the files provided with Host On-Demand. Creating your own files provides users with an easy way of starting a session and allows you to create customized sessions without having to go through the configuration windows.

You can find sample HTML files, session1.html and session2.html, in the **doc/samples/html** directory.

Session1 and session2 do not support new functions added to Host On-Demand V5. Use the Deployment Wizard instead.

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

- Creating an HTML file to bypass logon and start a configured session
- Creating an HTML file to configure and start a session
- Disabling functions through HTML files
- Creating buttons for sessions

Creating an HTML file to bypass logon and start a configured session

- Session1 and session2 do not support new functions added to Host On-Demand V5. 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.

Creating 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.SessionLaunch
<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 an HTML file to configure and start a session

- Session1 and session2 do not support new functions added to Host On-Demand V5. Use the Deployment Wizard instead.
- A pre-configured session is not required. An HTML file created by these steps configures and launches a session.
- You cannot use these steps to configure and launch a printer 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.

Disabling functions through HTML files

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

Configuring SSL

If you have clients outside your firewall connecting to any telnet server or Host On-Demand Redirector inside your firewall, you should configure SSL connections to ensure your data is secure. To configure SSL for servers and clients:

1. Obtain or create certificates for servers
2. Make server certificates available to clients
3. Configure clients to use SSL
4. Obtain or create certificates for clients needing to provide client authentication.

Configuring SSL on clients

Download clients

You can configure security on the client workstation or from the Administrator window. If you are configuring security on the client workstation, perform only steps 4 through 8.

To configure SSL for clients:

1. Open the Administration window (HODAdmin.html) and log on as the administrator.
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 (SSL).
6. To enable server authentication, click Server Authentication. Read about known security limitations when using the Internet.
7. To use client authentication, click Send a Certificate.
   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 be prompted each time the server requests a client certificate, click Prompt Each Time.
8. Click OK.
9. If clients will use secure sessions to the Host On-Demand server, click the Redirector tab.
   - If you are creating a new 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.

Locally installed clients

At the client workstation:

1. Click Start > Programs > IBM Host On-Demand > Host On-Demand.
2. Right-click the appropriate session icon, then click Properties.
3. Click the Security tab and then click Enable Security (SSL).
4. To enable server authentication, click Server Authentication. Read about known security limitations when using the Internet.
5. To use client authentication, click Send a Certificate.
   To specify a default location for the client certificate, enter a URL or path and filename. The URL protocols that can be used depends on the capabilities of your browser. Most browsers support http, https, ftp, and ftps.
   To be prompted each time the server requests a client certificate, click Prompt Each Time.

Setting security on the Redirector

To use secure sessions on a Host On-Demand Redirector, you must set a security level on the port

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

- Server authentication

Starting the Deployment Wizard

Use the Deployment Wizard to create a client HTML file that can be downloaded to start a session. The client HTML file can be used in to access the configuration server, but it's not required. The Deployment Wizard takes you step-by-step through the decision making process necessary to configure and deploy your Host On-Demand sessions. It replaces session1.html and session2.html provided in previous releases.

To start the Deployment Wizard from the Start menu, click Programs > IBM Host On-Demand > Administration > Deployment Wizard. To run the wizard from the CD, insert the CD into the system and select **Run Deployment Wizard** from the Welcome screen.

There are several advantages to using the wizard for creating client HTML files: you don't have to remember all of the parameter names, more options are available, and it's easier to update the client HTML files.

Many of the options available in the Wizard are not available from the Administration window. For example:

Accessing configuration information
: Choose where the client HTML file accesses configuration information: the server or the HTML file.

Cached client options
: Choose whether or not users should cache the client and configure cached client options.

Automatic logon for users
: Add user IDs and passwords so users don't have to log on.

Display options
: Choose the window size of the applet and if session icons are displayed in the client window or as a grid of buttons.

Set preloads
: Select functions to download when the applet is downloaded.

Set run-time options
: Configure and start a session to set options that run as part of the session, for example macros, keyboard settings, and client authentication.

Running the wizard from a Windows installation

The Deployment Wizard runs on Windows Operating Systems only. When you install Host On-Demand on Windows, the wizard is installed also and can be started from the Start menu. Or, you can run the wizard from the CD. The recommended way is to run the wizard from an installation, not the CD. When you run the wizard from an installation, the files created by the wizard are automatically saved to the correct location and no further action is necessary. Users simply load the client HTML file you created to start a session:

```
http://hod_server/hod_alias/client_HTML_name.html
```

server_name is the host name or IP address of the Host On-Demand server, *hod_alias* is the alias (or path) of the published directory, and *client_HTML_name* is the file name of the client HTML file.

Each time you run the wizard, a directory, a text file, and two HTML files are created. If you are not using the Configuration Server, object files and a configuration file are created for every defined session. You can copy the client HTML files from one installation to another. For example, if I create a client file named newgroup.html, the wizard creates two files, newgroup.html and autonewgroup.html, and a directory named /HODData/newgroup/ in the publish directory. The auto*.html file is required to bookmark a session.

To use these client HTML files on another operating system, move both HTML files and the /HODData/newgroup/ directory, including the files, to the publish directory of another installation. Directories are case sensitive and must be maintained.

Transfer files in binary when transferring to the host system. For MVS and UNIX operating systems, set file permissions for those files to 666, for example, **chmod 666 newgroup.html**.

File extensions for HTML files transferred to an MVS host system must be changed to html.ascii. File extensions for text files located in the HODData subdirectories must be changed to txt.ascii.

Running the wizard from the CD

If you are running the wizard from the CD, it generates one zip file in the directory that you choose. Extract the files from the zip file to the publish directory for the Host On-Demand server.

Editing client HTML files

Files created with the wizard should be updated in the wizard. If you create a file with the wizard, manually edit the file and then bring it back into the wizard, your changes might be gone. The wizard reads the information from the file and creates a new client HTML file. Only the information for the options contained in the wizard are read into the new file.

Using the Configuration Server

If you choose to use the configuration server when creating a client HTML file, configuration information, including sessions, is accessed from defined users on the configuration server. Every time you load the client HTML file, the configuration server must be accessed.

If you choose not to use the configuration server, configuration information is defined in the client HTML file. Sessions are configured while running the wizard and included in the HTML file. Therefore, the client HTML file does not require accessing the configuration server but any updates must be made through the wizard.

Selecting preloaded functions

Using the wizard, you can determine what functions should be preloaded. Preloaded functions are functions that are downloaded as part of the initial download. Other functions are downloaded when needed. This creates a smaller download client file and increases performance.

Once preloaded functions are downloaded, available functions are determined by what is enabled and disabled when the user logs on. If disabled functions are included as preloaded functions, they are still downloaded when users start a session. However, users won’t have access to them until the function is enabled.

Choosing the cached client

The cached client is cached on your local disk the first time you download it. The next time you start a session, the applet does not need to be downloaded from the server but checks the server to see if any of the components on the server are more recent than those in cache. If not, the cached client components are loaded from your cache. If there are later versions of the components on the server, the new versions are downloaded and replace the versions on your workstation. If you choose to use the cached client, the wizard takes you through the available options.

Disabling functions

Disabled functions are functions that users cannot 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. This option is available only when you are creating client HTML files that don’t require accessing the configuration server.

Session 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 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	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 ResQ!Net. 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: *SessionName*
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 delimitter 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 S/390 or AS/400 to which the session will connect.	A supported host code-page	037
Locale	Sets the locale.	xx_YY xx = language code YY = country 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
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

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
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
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 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 tl 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 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? entr 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_ 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_ entry in the PDT. If the entry is not found the default value, false, is used.
ignoreFFFirstPos	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_PO 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 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 ir 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	0, 1, 2	0

	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.		
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 and the respect country's default ASCII code-page for oth countries.
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

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 AS/400 file that can be used to format the data for this device.	String	NONE
customizingLibrary	The name of the AS/400 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	00

		06 - B5 07 - Continuous 80 column form 08 - Continuous 132 column form 0E - A3 0F - B4 10 - Ledger	
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, HACLTAU, 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	<none>	URL, or file name relative to code base

	document contains the word **upgrade**, the user is upgraded		

Host On-Demand Service Manager

The Host On-Demand Service Manager provides support for persistent user configuration, error logging, and the Redirector. The Service Manager is a Java application and must always be running.

When you log on as the administrator, you may see the following error message:

```
The Host On-Demand client is unable to contact the Host On-Demand Service M
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. Please contact your system administrator.

This message indicates the service manager is not running on the server.

- On Windows NT, the service manager runs as an NT 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) 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.

In other environments, you must manually start the service manager as a Java application. Sample command files for OS/2, NetWare, AIX, UNIX, and AS/400 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 server:

1. Click Start > Settings > Control Panel.
2. Open the Services folder.
3. Highlight IBM eNetwork 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 **Jre** task and then click End Task.
3. Restart the Service Manager through Host On-Demand Administration in the Start menu.

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/hos
   ```

   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.

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 Services tab and then click Server Log.

To view a service trace file after tracing has been started, click the Services tab 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. Click Users/Groups.
2. Right-click a user and select Trace Facility.

To refresh the messages in the console, click File > Refresh.

Related topics

- Setting trace levels
- Log and trace messages

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.

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

Host On-Demand Redirector

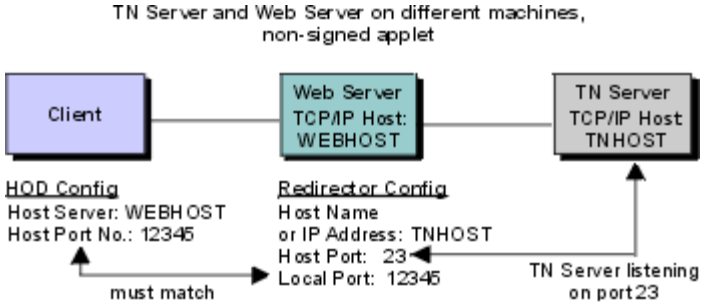
- Adding a host to the Redirector.
- Changing the session configuration to connect to the Redirector instead of the host.

The Redirector allows clients to connect to telnet servers that are not installed on the same system as the Host On-Demand server. On Windows NT and AIX, it also 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 a host as a Redirector

To add a host to the Redirector:

1. Click Services in the Administration window.
2. Click Redirector Service.
3. Click Add.
4. Enter the target host's destination address. Make any necessary changes to the port numbers or security.
5. 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. The local port is part of the Redirector's intercept procedure, which allows an emulator to connect to telnet servers that do not reside on the same host as the Web server.

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

Changing a host defined to the Redirector

To change a host that has been defined to the Redirector:

1. Click Services in the Administration window.
2. Click Redirector Services.
3. Highlight the host configuration you want to change.
4. Click Change.
5. Make the necessary changes.
6. 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. The local port is part of the Redirector's intercept procedure, which allows an emulator to connect to Telnet servers that do not reside on the same host as the Web server.

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 Services in the Administration window.
2. Click Redirector Service.
3. Select the host configuration you want to delete in the Redirector window.
4. Click Delete, then confirm.

Related topics

- Redirector overview
- Adding a host to the Redirector

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

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 statements.
- Executable 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 variable (CSV)
    - Lotus 1-2-3 (WK1)
    - Microsoft Excel (BIFF3 and BIFF4)
    - HTML
- 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 AS/400 JDBC driver is shipped and packaged with Database On-Demand. Other user-installed JDBC drivers can also be used.

If you are using a proxy server to connect to an AS/400, you can decrease the download time when loading the Database On-Demand applet. To do that, edit the HODDatabase.html applet and replace the following jar and cab file names:

Replace	With
hoddba.jar	hodpxdba.jar
hoddba.cab	hodpxdba.cab

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 statements

Saved SQL statements can be distributed to a user or a group of users. You can simply select the saved SQL 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.

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

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 AS/400 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 AS/400. 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 (AS/400): 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

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. When a user is a member of multiple groups, the most-permissive option is granted.

When options are modified for a selected user, the new settings override settings for the group or groups to which the user may belong. This gives the administrator the ability to allow or restrict certain functions at the user level.

Individual options are grouped into the following categories:

General

- **Allow creating SQL Statements**
  Allows you to create new SQL statements.

- **Allow saving SQL Statements**
  Allows you to save SQL statements that you create or modify. This option is valid only if Allow creating SQL Statements is selected.

- **Allow deleting SQL statements**
  Allows you to delete previously saved SQL statements. You can delete only your own saved SQL 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

- **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

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 see general options page**
  Allows modification of the General options.

- **Allow user to see tables options page**
  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**
  Allow the User options.

Related topics

- Database On-Demand Overview

Statements

Click Statements to manage SQL 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 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 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 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 Administer Statements can rename a saved SQL statement. After a statement is renamed, the original statement name is no longer valid.

To rename a saved SQL 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 statement. After a statement is deleted, the original statement is no longer accessible. The delete action is final.

To delete a saved SQL 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 SQL statements

Database On-Demand provides an interface for creating, modifying, and running SQL statements. A set of tabbed tabs is used to guide you through the process of building and executing a valid SQL statement.

The following tabs are used to build and execute the SQL statement:

- Logon
- Tables
- Join
- Condition
- Columns
- Sort
- Output
- SQL
- Results
- Insert
- Update

If you see this message when logging on:
`java.lang.NoClassDelFoundError:com/ibm/as400/access/AS400JDBCStatement`
you must rename the Netscape jit*.dll file so that it is not a dll file type. This file is located in the \program files\netscape\communicator\program\java\bin\ directory.

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 AS/400 Toolbox for Java JDBC driver requires:

  `jdbc:as400://`*`as400name`*

  where *as400name* is the fully-qualified network name of the database host.

  To use a proxy server when connecting to the AS/400 database, include the proxy server name and port number:

  `jdbc:as400://`*`as400name`*`;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.

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.
2. Select the table(s) you want to access. You can select multiple tables.
3. Click Next.

Click View schema(s) to add tables from additional schemas. A schema is similar to a database or library. For AS/400 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 variables**
  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(BIFF3)**
  Select Microsoft Excel(BIFF3) if you are using the file with a version of Microsoft Excel that supports importing of data in BIFF3 format.

- **Microsoft Excel(BIFF4)**
  Select Microsoft Excel(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.

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.

Getting started with Database On-Demand

The Database On-Demand client lets you extract data from an AS/400 database for use in a workstation application.

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.

The Database On-Demand window opens and you can start working with SQL statements. This window displays a view of all your previously-saved statements and allows you to create, open, run, and delete existing SQL statements.

Creating a new SQL statement
Opening an existing SQL statement
Running an existing SQL statement
Deleting an existing SQL 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 statement

To create a new SQL statement and save the statement for later use:

1. Click New. The logon tab displays.

2. Type the URL for the AS/400 database:

   `jdbc:as400://as400name`

   To use SSL when connecting:

   `jdbc:as400://as400name;secure=true`

   To use a proxy server when connecting to the AS/400 database, include the proxy server name and port number:

   `jdbc:as400://as400name;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 (Table, Join, Condition 1, Columns, and so on). Use these tabs to create your SQL statement.

7. When you are satisfied that the SQL statement is correct, click Save SQL on the SQL tab to save the statement. Once saved, this SQL statement appears as an entry on the Database On-Demand window for later use.

Opening an existing SQL statement

You can view and edit the options used to create an existing SQL statement. This allows you to make changes to commands without reconstructing them each time. For example, if you are running a 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 statement:

1. Click the icon for the SQL 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 connected, a series of new tabs appears at the top of the Logon tab (Table, Join, Condition 1, Columns, and so on). These tabs contain the information used to create the original SQL statement. You can change the supplied information, execute the new SQL statement, and save the results.

Running an existing SQL statement

To run an existing SQL statement:

1. Click the icon for the SQL statement you want to execute.

2. Click Run.

3. Enter your ID and password (if they were not saved with the selected SQL statement). Type the information and click Connect. If you saved the ID and password with this SQL statement, skip the next step.

4. Your SQL statement results are displayed or sent to a file. (See Output tab for more information.)

After running the SQL 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.

Deleting an existing SQL statement

You may need to remove SQL statements that have been previously saved. You can delete an existing SQL statement but remember that once statements are deleted they cannot be recovered; you must build a new statement.

To delete an existing SQL statement:

1. Click the icon for the SQL 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

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

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, **AS/400 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 or Apply.

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.

Related topics

- Database On-Demand overview
- Database On-Demand SQL statements

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 **lib\licusemgmt.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.

Related topics

- Enabling license usage counting
- Considerations for selecting a report interval time

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 are very small as well as the CPU resources required to count the number of workstations.

- 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.

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 tab of 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 Services in the Administration window.
2. Select Directory Service (LDAP).
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 AS/400 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 of more subgroups as children and each subgroup inherits all of the sessions defined by the parent group. A user can be an immediate member of any one group and inherits sessions from all the groups in its inheritance tree. This means that you can define sessions in a high-level group for a large number of users and subgroups and then customize them in lower-level groups for smaller numbers of users. It also means that no user can belong to more than one group.

Will migrating to LDAP change my present group structure and user configurations?

Yes. Because your Host On-Demand private data store is not arranged hierarchically, migrating your configuration information to an LDAP directory changes the relationship between your users and groups. Specifically, all groups and their sessions become children of the root group of the LDAP directory and all users become members of one of the groups they were members of before migration (refer to the migration log for details). Also, because of this change, users that are members of multiple groups will lose configuration information as a result of migration.

What happens if I choose not to migrate my configuration information?

None of the users, groups, and sessions that are defined in the private data store will be accessible from the logon window or the administration window. If it does not already exist, Host On-Demand will create a single administrator User ID named "admin" with a password of "password."

What happens to the configuration information in the private data store when I migrate?

It is preserved and is not modified by the migration process. However, it does not reflect the latest updates either. When you use an LDAP directory, changes to configuration information will only be updated in that LDAP directory.

Once I have migrated and started using LDAP, how do I switch back to using the Host On-Demand private data store?

Clear the Use Directory Service (LDAP) box on the Directory tab, and click Apply. This will disable use of the LDAP directory and Host On-Demand will begin retrieving user and group information from the private data store.

Is there anyway to migrate my configuration back to the Host On-Demand private data store?

No, migrating from an LDAP directory to the Host On-Demand private data store is not supported.

Related topics:

- Setting up and using LDAP
- Specifying the LDAP directory information
- Migrating to an LDAP directory

- Understanding directories

Server authentication

When you define a secure connection, Host On-Demand offers three options on the Security tab: Enable Security (SSL), Server Authentication (SSL), and Send a Certificate (client authentication). to enable server and client authentication you must first enable SSL.

The Security (SSL) option creates a standard SSL connection; that is, 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. However, this option by itself does not guarantee that the client is communicating with the correct server.

To illustrate the risks involved with this level of security, consider the following scenario. There are two servers, **S1** (hod.S1.com) and **S2** (hod.S2.com), and one client, **C**. Both servers have valid certificates from a CA that the client trusts. C wants a secure session with S1, but S2 wants to eavesdrop on their communication, and is physically located in such a place that it can do so. The scenario goes as follows:

1. C sends a request for an SSL session to S1.
2. The request (and all subsequent traffic) actually goes through S2. Instead of forwarding C's request to S1, S2 responds directly to the request by sending its own certificate to C.
3. C receives S2's certificate and checks its list of trusted CAs. Since S2's certificate is signed by the same CA as S1's certificate, C accepts the certificate and creates a secure session with S2.
4. Having completed the secure session with C, S2 requests and creates its own SSL session with S1.
5. From this point, C sends encrypted information to S2. S2 decrypts the information, re-encrypts it, then sends it to S1. 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, S2 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. C sends a request for an SSL session to S1.
2. The request (and all subsequent traffic) actually goes through S2. Instead of forwarding C's request to S1, S2 responds directly to C's request by sending its own certificate to C.
3. C receives S2's certificate and checks its list of trusted CAs. Since S2's certificate is signed by the same CA as S1's certificate, C accepts the certificate and creates a secure session with S2.

4. After the secure session has been completed, but before any real data has been sent or received, C 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, C knows that the connection should not continue and disconnects it.

Related topics

- Obtaining a server certificate
- Making server certificates available to clients

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 NT only)
- Certificate Management (Windows and AIX only)

Related topics

- 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 3 Public Primary CA
- 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 NT, 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/*server_dir*/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 NT, 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/*server_dir*/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:

- 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 NT, 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. 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 NT, 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/*server_dir*/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:

- 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:

- Server authentication

Running Certificate Management on AIX

Before running Certificate Management on AIX, you must be in the hostondemand/bin directory, and the JAVA_HOME environment variable must be set to the full path to your Java installation. For example, if you expanded the hod40srv.tar file to the /usr/opt/hostondemand directory and 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
```

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 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. 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

- 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 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.

When a server requests a certificate, the client has the option to send a certificate or attempt to connect without it. The server attempts authentication when the client sends a certificate, and makes a 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.

To configure client authentication:

1. Obtain certificates for clients.
2. Send certificates to clients.

   Note: Make sure that sending the certificates does not compromise them.
3. Configure clients to use client authentication.

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

Related topics

- Server authentication

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.
6. Click Enable Security (SSL). Click Yes for Send a Certificate. Optionally, select a location for the certificate. This will be the default location for the selected user or group. If you do not want the location changed, click Lock. Otherwise, users can choose the certificate location. If you click No for Prompt Each Time, the user is prompted for a certificate only once per browser session.
7. Click OK.

On the client:

1. Right-click the session icon, then click Properties.
2. Click the Security tab.
3. Click Enable Security (SSL).
4. Click Yes for Send a Certificate. Optionally, enter a default location for the certificate. The location can be changed when the user is prompted.
5. Click No for Prompt Each Time if you don’t want to be prompted for a certificate and password every time a server requests one.
6. Click OK.

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

Related topic:

- Client authentication

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, keep this option to a limit. 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 export the certificate into a PKCS12 (.p12 file type) file format and save it on their workstations to be used for client authentication. Certificates exported from a 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 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/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

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:

- Server authentication

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

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

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.

Printer sessions run through a browser and use a Java interface in the same way as display sessions; as a result, they cannot use the drivers provided by the workstation's native operating system. Instead, Host On-Demand uses a **printer definition table (PDT)** to format the data and send it to the printer as text and printer commands.

PDTs provide great flexibility because you can customize them to produce the printed output you want without modifying the host application. 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.

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 AS/400 as a print job that can be printed on any AS/400 printer. If the job is directed to a Host On-Demand 5250 printer session, it will print on the printer specified for that session. Host Print 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 AS/400 print-data stream to ASCII just before it is sent from the AS/400 to the PC printer. Having the conversion done on the AS/400 ensures that most of the print processing is not done there, not on the workstation.

The ASCII print-data stream is suitable for many IBM and non-IBM printers; it uses AS/400 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 AS/400 to do AFP-to-ASCII transform, which Host On-Demand also supports. The ASCII data stream is passed through the emulator 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.

For more information about the host print transform, refer to:

- Host Printing Reference
- *AS/400e series Printer Device Programming Version 4* manual.

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.

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\CommandFilesdirectory.
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)

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. 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.

For more information, refer to the Host Printing Reference

Printer tab

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.

Notes:

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.

4. VT sessions do not use a PDT. 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.

Print Destination
Choose whether the output should go to a printer or to a file

Printer Name
Type the name of the port for the printer you want to use. On Windows workstations, you can type the UNC name of a network printer in either of two formats:

\\server_name\printer name
\\server's_host_name_or_IP_address\printer name

For example, if you are configuring a printer on Windows 95 or NT, type a port name such as LPT1. If you are configuring a printer on UNIX, type a device name such as /dev/lp0.

Select Printer
Click this button to see the Printer Selection dialog window where you can specify a defined printer.

File Path and Name
When the print destination is a file, type the path and name of the file; if either does not exist, it is created.

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 name is numerically incremented for each print job. For example, if you name the file prt*.file, the first file will be named prt000.file, the next will be named prt001.file, 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. Host On-Demand appends numbers to the file-name, starting at 000 (prt.file.000, prt.file.001, and so on).

If you choose Separate = 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.

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 have jobs appended to each other in one file.

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.

Use 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. The default is 25. A value of 0 disables the timer and a message never appears.

Advanced Options (3270)

Advanced options (3270)

The Advanced Options window lets you 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:

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

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

Characters per inch

Specifies the number of characters printed per inch. The choices that appear are defined in the PDT.

The default value is taken from the DEFAULT_CPI? entry in the PDT if this entry exists.

Lines per inch

Specifies the number of lines per inch. The choices that appear are defined in the PDT.

The default value is taken from the DEFAULT_LPI? entry in the PDT if this entry exists.

Maximum lines per page

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

The default value is taken from the MAXIMUM_PAGE_LENGTH entry in the PDT. If the entry is not found, 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.

The default value is taken from the MAXIMUM_PRINT_POSITION entry in the PDT. If the entry is not found, the default value, 132, is used.

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.

The default value is taken from the COMPRESS_LINE_SPACING? entry in the PDT. If the entry is not found, the default value, No, is used.

Print nulls as spaces

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

The default value is taken from the OVERRIDE_FORMATTED_PRINT? entry in the PDT. If the entry is not found, the default 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.

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, the default 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.

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, the default 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.

The default value is taken from the IGNORE_FORM_FEED_AT_FIRST_POS? entry in the PDT. If the entry is not found, the default 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.

The default value is taken from the FORM_FEED_TAKES_POSITION? entry in the PDT. If the entry is not found, the default 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.

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, the default value, Column 1 only, is used.

Ignore attributes

This option applies only to LU Type 3 sessions.

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

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	**axxxxxaxxxxx**axxxxx	**axxxxxaxxxxxa**xxxxx

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).

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.

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, though 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 LU Type 1 sessions.

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.

Tractor feed

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.

Printer-font code-page

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.

The default is 850 for Latin-1 countries and the respective country’s default ASCII code-page for other countries.

Inactivity time (secs)

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

The default value is 25 seconds. A value of 0 disables the timer; a value below 11 sets an interval of 10 seconds; the maximum value is 255.

Selecting a Windows printer to use with a host printer session

To select a Windows printer to use with a 3270 printer session:

1. Open your client window.
2. Right-click on the 3270 printer session icon that you want to use with a local Windows printer and select Properties.
3. Click the Printer tab on the 3270 printer session notebook.
4. Click Select Printer.
5. Click Continue on the window with the message "Windows printer selection requires approximately 60k bytes of software to be downloaded" to download the necessary software and select a Windows printer.

   If you receive the error message "Unable to download file from http://*host_name*/hod/hodpdt.properties." the hodpdt.properties file could not be found in the publish directory and the Windows printer selection will not be updated. For more information, view "Customizing hodpdt.properties and hodmodel.properties"

6. Select a Windows printer from the list of installed Windows printers that were detected in the Printer Name field. The appropriate associated printer driver is inserted in the Printer Driver field automatically. If you did not receive the list of printers you expected view "Customizing hodpdt.properties and hodmodel.properties" for more information.
7. Click OK to accept the PDT definition that Host On-Demand matched to the printer driver.
8. Click OK on the Printer tab on the 3270 Printer session notebook to finish. The Printer Definition Table field is updated with the appropriate PDT definition, and the Printer Name is updated with the name of the Windows printer.

To select a Windows printer to use with a 5250 Printer session:

1. Open your client window.
2. Right-click on the 5250 printer session icon that you want to use with a local Windows printer and select Properties.
3. Click the Printer tab on the 5250 printer session notebook.
4. Click Select Printer.
5. Click Continue on the window with the message "Windows printer selection requires approximately 60k bytes of software to be downloaded" to download the necessary software and select a Windows printer.

If you receive the error message "Unable to download file from http://*host_name*/hod/hodmodel.properties." the hodmodel.properties file could not be found in the publish directory and the Windows printer selection will not be updated. View "Customizing hodpdt.properties and hodmodel.properties" for more information.

6. Select a Windows printer from the list of installed Windows printers that were detected in the Printer Name field. The appropriate associated printer driver is inserted in the Printer Driver field automatically. If you did not receive the list of printers you expected view "Customizing hodpdt.properties and hodmodel.properties" for more information.

7. Click OK to accept the Model definition that Host On-Demand matched to the printer driver.

8. Click OK on the Printer tab on the 5250 printer session notebook to finish. The Printer Model field is updated with the appropriate Model definition, and the Printer Name is updated with the name of the Windows printer.

Related topics:

- Host Printing Reference
- Customizing hodpdt.properties and hodmodel.properties
- Printer Selection

Customizing hodpdt.properties and hodmodel.properties

With Host On-Demand 5.0, clients running on Windows workstations can use a locally installed printer driver to print host files. Host On-Demand uses a properties file called *hodpdt.properties* to identify a local Windows printer with a Printer Definition Table (PDT) file for a 3270 session, and a *hodmodel.properties* file with a Printer Model for a 5250 session. Sample *hodpdt.properties* and *hodmodel.properties* 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.

Customizing hodpdt.properties

The *hodpdt.properties* 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.properties* file using an ASCII text editor.

Sample hodpdt.properties 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.properties

The *hodmodel.properties* 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.properties* file using an ASCII text editor.

Sample hodmodel.properties 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 topics:

- Host Printing Reference
- Selecting a Windows printer to use with a host printer session
- Printer Selection

Printer selection

Select a Windows printer that is installed on your Windows workstation to be used with your 3270 or 5250 printer session by setting:

Printer Name

Displays the list of Windows printers detected on the Windows workstation. The printers detected can be locally installed (directly attached) or accessible across a network. Select one printer from the list.

Printer Driver

Displays the printer driver associated with the currently selected *Printer Name*. The driver is matched to an entry in the pdt.properties table (for 3270 sessions) or model.properties (for 5250 sessions) for an appropriate PDT (for a 3270 session) or Model (for a 5250 session) that formats the host print output for the session.

Clicking "OK" updates the Printer Definition Table or Printer Model field on the Printer tab in the 3270 Printer or 5250 Printer session notebook with the name of the selected Windows printer. If there is no match for the printer driver in the hodpdt.properties table (for a 3270 session) or the hodmodel.properties table (for a 5250 session), the default table entry is used. If there is no matching table entry for the printer driver and no default table entry, no new PDT or Model is selected and the Printer Definition Table or the Printer Model field is not updated.

Related topics:

- Customizing hodpdt.properties and hodmodel.properties
- Selecting a Windows printer to use with a host printer session

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.

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

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 it. The new session has the same configuration as the session from which you copied.
2. Right-click the new icon and click Properties. Make your changes.
3. If you want to make another copy, right-click in an empty area of the window, then click Paste.

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.

The Active Sessions area

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.

Logging off

Click Log Off to close the Client window. Changes you make to host sessions are not saved until you log off or close the browser.

Closing the Client window also ends all your host sessions.

Related topics

- Adding sessions

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

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

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, and the default directory is the one in which your browser is installed.
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 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 always uses 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 Basic ASCII text mode PDT.

- **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.

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

Starting sessions with bookmarks or icons

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.
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 AS/400

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 or Host On-Demand *Specially Developed for On-Demand Server*,

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.

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 do not always appear on the screen.

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 ASCII 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 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.

ASCII elements

For ASCII sessions, you can define these elements.

The base attributes include formatting attributes, such as reverse, underline, and bold, when the session is in base color mode.

The extended attributes define the color selections of the ASCII machine mode.

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
- VT340 graphics colors defines the color selections available for VT340 graphics (VT340 only).

Related tasks

- Understanding session colors
- Using the host session default colors

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 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.

Remapping the keyboard

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.

Assigning keys to a function

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 using the Alt, Ctrl, and Shift keys to a function (for example, Alt+F1 or Ctrl+Alt+Q,).

   
   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 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.

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.

For the 3270 and 5250 emulators, the Ctrl key default mapping is Enter. 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 Enter to any other key.

Related topics

- Key definitions

Key definitions

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

- The Copy function is 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, Copy duplicates the entire session window.
- Copy does not duplicate host attributes such as color and intensity.

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-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 upon 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.

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.

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

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 identically 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.

Host Print - Informs the host system that the operator wants to print the contents of the present display.

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.

Note: 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.

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

Page Up - Displays the previous page.

Page Down - Displays the next 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.

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

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 mapped$_1$	X	X	X	X
Alternate View(note$_6$)	Ctrl+F3	X	X		
Attention	Not mapped$_1$	X	X		X
Backspace	Backspace	X	X	X$_2$	X
Backtab	Shift+Tab	X	X	X	X
Backtab Word	Ctrl+ <	X	X		X
Beginning of Field	Not mapped$_1$	X			X
Clear	Esc	X	X	X$_2$	X
Copy$_5$	Ctrl+Insert	X	X	X	X
Cursor Down	Down arrow	X	X	X$_2$	X
Cursor Left	Left arrow	X	X	X$_2$	X
Cursor Right	Right arrow	X	X	X$_2$	X
Cursor Up	Up arrow	X	X	X$_2$	X
Cut$_5$	Shift+Delete	X	X		X
DBCS Input(note$_6$)	Not mapped$_1$	X	X		
Delete Character	Delete	X	X	X$_{2,3}$	X
Delete Word	Ctrl+Delete	X	X	X	X
DUP Field	Not mapped$_1$	X	X		X
>Enter	Enter		X	X	X
Enter	Ctrl	X			
End Field	End	X	X	X$_{2,3}$	X
Erase Field	Not mapped$_1$	X	X		X
Erase EOF	Not mapped$_1$	X	X		X
Erase Input	Not mapped$_1$	X	X		X
Field Exit	Ctrl+Enter		X		
Field Mark	Shift+Home	X	X		
Field Minus	Not mapped$_1$		X		
Field Plus	Not mapped$_1$		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	X[4]	X
Graphic Cursor	Alt+PF12	X			
Help	Not mapped[1]		X		
Home	Home	X	X	X[2,3]	X
Host Print	Ctrl+Pause		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
PA1	Not mapped[1]	X	X		X
PA2	Not mapped[1]	X	X		X
PA3	Not mapped[1]	X	X		X
Page Up	Page Up	X	X	X[2,3]	X
Page Down	Page Down	X	X	X[2,3]	X
Paste[5]	Shift+Insert	X	X		X
Reset	Not mapped[1]	X	X	X	X
Rule	Ctrl+Home	X	X	X	X
SO/SI Display(note[6])	Ctrl+F1	X	X		
System Request	Not mapped[1]	X	X		X
Tab Field	Tab	X	X	X[2]	X
Tab Word	Ctrl+ >	X	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.

Related topics

- Remapping the keyboard
- Key definitions

Key Assignment

Category

Select the category of function you want to work with. For example, menu item, host function, character, and so forth

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.

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.

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.

Related topics:

- Remapping the keyboard
- Specifying a key as repeating or non-repeating

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-recomment 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-recomment 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 currupted, 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.

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 so that it repeats, 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.

Related topics

- Key definitions

Cut, copy, paste

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

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.

Cut

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.

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.

Copy

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.

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.

Paste

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.

- 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.

Advanced Cut, Copy, and Paste

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.

Paste tab

Field Wrap

If you activate the Field Wrap checkbox, the data that would fall onto a protected field is 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*.

For data that contains end-of-line (EOL) indicators, the information after the first EOL indicator is lost, unless you enable the Line Wrap function. The Edit > Paste Next menu item is not enabled after the EOL indicator is encountered. However, the Edit > Paste Next menu item is always enabled when an end-of-screen is encountered.

If you leave the checkbox unchecked, any data that falls on a protected field is lost.

Line Wrap

If you activate the Line Wrap checkbox, the Line Wrap function recognizes end-of-line and end-of-screen indicators and continues 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

If you activate the Paste to marked area checkbox, 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

If you activate the Stop pasting when protected field encountered checkbox, your data is 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

If you activate the Advance to next tab stop radio button, you can 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:

If you activate the Replace with: radio button, you can 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)

If you activate the Paste data to fields radio button, 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.

Cut/Copy tab

If you activate the Cut/Copy only if a trim-rectangle is marked checkbox, the Edit > Copy, Edit > Copy Append, and Edit > Cut functions are disabled until you draw a trim-rectangle or until you use the keyboard to select a block of text. In other words, if you select this function, 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, and Edit > Cut functions cut or copy the entire screen or the contents of a trim-rectangle, if one is drawn.

Trim tab

Trim Rectangle sizing handles

If you activate the Trim Rectangle sizing handles checkbox, you can 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

If you activate the Trim Rectangle remains after edit function checkbox, the trim-rectangle

remains 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.

Related topics

- 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

Setting 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 default options in two ways:

- 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 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.

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.

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.

file transfer destination address
This option specifies the actual final destination address of the host to be used for the file 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.

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 countries and Taiwan and Korea. 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 countries and Taiwan and Korea. 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'OF') 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 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.

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 countries and Taiwan and Korea. 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 countries and Taiwan and Korea. 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 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 countries and Taiwan and Korea. 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 AS/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 "AS/400 Source physical file". This option is applicable only for the files in the QSYS library file system.

DTA
This option specifies the AS/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 "AS/400 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 transfering files to the AS/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 countries and Taiwan and Korea. 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 recieve text files (saved in EBCIDIC) 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'OF') 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 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 AS/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 "AS/400 Source physical file". This option is applicable only for the files in the QSYS library file system.

DTA
This option specifies the AS/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 "AS/400 Physical data file". This option is applicable only for the files in the QSYS library file system.

SAVF
This option specifies the AS/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 "AS/400 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 transfering files to the AS/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.

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.

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.

Transferring files

1. Start a host session.
2. Make sure that the correct host system and other options have been specified.
3. Click Transfer > 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 filenames 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.

File transfer overview

You can transfer files between your workstation and S/390 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 S/390, file transfer uses the IND$FILE (SBCS) or APVUFILE (DBCS) program; for AS/400, 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 the Host On-Demand Installation and Planning Guide for details.

- Transferring files
- Changing a file transfer list
- Setting default transfer options

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.

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. Check 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, click Macro Manager on the tool bar, select a macro from the Macro selection list and then click Edit.

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.
2. Click Existing.
    - To replace the macro with a new one, click Overwrite.
    - To add keystrokes to the end of the macro, 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 the procedure you want to record.
    - 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.

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. However, 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 three elements. Each tab represents an element:

Macro
: 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.

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.

Related topics

- Using the Macro Editor (an overview)

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.

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.

Express Logon Feature

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.

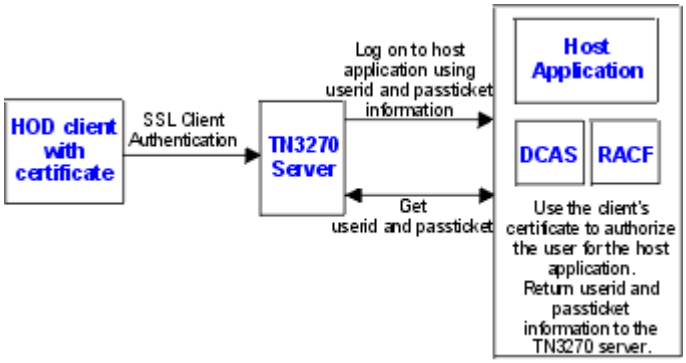
Some configuration needs to be done on the telnet servers and on the OS/390 system that you are accessing. The information in this help describes only what you need to configure for Host On-Demand. Refer to the following telnet server's documentation and OS/390 documentation for configuration information:

- 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*

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.



Supported servers

Express Logon is supported on the following servers. Refer to the product's documentation for configuration information.

- Communications Server for AIX V6.0.0.1 with PTF
- Communications Server for OS/2 V6.1
- Communications Server for Windows NT V6.1.1
- Communications Server for OS/390 V2R10 with Information APAR
- OS/390 V2R10 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.

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.

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 OS/390 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.

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.

  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 **$USR.ID$**.
  9. Click Save.
- If you are connecting to a tn3270 server through a Redirector, the security option for the Redirector configuration must be set to Pass-through.

Distributing the 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.

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.

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

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.

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.

A data extraction is intended for host-system 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.

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 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.

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.

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 and Host On-Demand V4 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.

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

Click Edit Code to directly edit the XML script. 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. You must fix any problems before the macro can be saved. Press Cancel to return to the Macro Editor without saving any changes.

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)

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.

General

Provides general information about the screen.

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
Check this option 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
Check this option if the selected screen is the last screen in the macro to be displayed. Only one screen can be identified as the exit screen. The macro stops playing when it comes to the exit screen.

Transient Screen
Check this option 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 which 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.

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.

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.

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 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.

By default, when the Macro Manager records a macro, the field counts descriptor is defined to identify the screen. If this is adequate, you don't need to make any changes on this tab. You can narrow down the list of possible matches following a given screen by defining a limited set of Valid Next Screens on the Links tab.

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

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. 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, and the string that was in your selected area will be entered in 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. If end row and end column are not specified, then absolute position is used. 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 when this option is not checked.

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 checked, the string defined by this descriptor must not be displayed on the session screen.


You can enter negative numbers for rows and columns. Negative numbers are virtual positions from the bottom row.

Cursor

Identifies the screen based on the position of the cursor. Specify the cursor position, or click the 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 checked, the cursor defined by this descriptor must not be displayed on the session screen.

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.

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 checked, the attribute defined by this descriptor must not be displayed 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 checked, the fields defined by this descriptor must not be displayed on the session screen.

Wait for OIA to become Uninhibited
If checked, the OIA must become uninhibited (able to enter keystrokes) before the actions will execute.

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.

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>).

- 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 or unmarks an area on the screen.

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 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. This function has no significance in regards to playback through a Host On-Demand emulator.

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.

Unwrap Text

Unwrap text in a field that spans multiple lines on the screen.

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

Encrypts the response for the prompt (for example, if the prompt is asking for a password

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.

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.

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.

Related topics

- Bidirectional language support
- Transferring files

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
- Command line

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 or unmarks an area on the screen.

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.

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.

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.

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 a browser are usually weakly encrypted. Certificates exported from Certificate Management or Certificate Wizard are strongly encrypted. This makes them more secure from unauthorized access, but they cannot be imported into most browsers. Use strong encryption when accessing certificates 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 a 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 (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.

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.

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.

To change the password or the encryption strength for the selected certificate, click 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

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

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.

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.

Message Help

Click on a message number to view an explanation of the message and any action you need to take.

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

ECL0001 Internal Emulator Class Library program error.

Explanation
The Emulator 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, following the directions in

the README file for reporting product problems.

ECL0002 An Emulator Class Library event error occurred.

Explanation
The Emulator 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 SSL 3.0 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 intialized.

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 is defined by INTERNET-DRAFT "TLS-based Telnet Security". Servers which support this function respond IAC DO STARTTLS during the Telnet negotiations. Host On-Demand has recieved 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 INTERNET-DRAFT "TLS-based Telnet Security". 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-based Telnet Security" 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 (SSL) on the Security configuration is Yes, verify that there is an available server within specified scope that supports SSL V3.

If there is an SLP AS/400 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 specifed scope that links to that AS/400.

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 AS/400 objects of the type *FILE are supported under the QSYS library file system. Also, among the AS/400 *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 transfering AS/400 SAVF files.

Explanation
For transferring SAVF files to the AS/400, 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 AS/400.

ECL0259 Unable to open the host file for writing.

Explanation
The host file cannot be 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 the AS/400. Also, if you get any of the following error messages when performing 5250 File Transfer, please refer to the Installation and Planning guide and make sure that the setup instructions were followed. 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 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 (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 th4e 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 SSL.

Explanation

In order to support SSL 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 SSL sessions.

User Action

If the Redirector is running on a platform that does not support SSL, then no action is necessary. If the Redirector is running on a platform that supports SSL, re-install the product. If the problem persists, contact an IBM service representative.

Printing a screen

To print your screen, click File > Print screen.

You can only print screens to printers installed on your desktop.

Print Screen requires a Java Virtual Machine (JVM) with full Java 1.1 support, which includes the Abstract Windowing Toolkit (AWT). If your browser does not have this support, the Print Screen selection is not available.

You can print the entire presentation space of your Host On-Demand window.

When you print a host graphics screen, the image is scaled to print on paper; therefore, it is possible that print quality may occasionally be degraded.

Understanding bidirectional language support (Arabic and Hebrew)

- 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

The bidirectional Text Assist Function is not supported for Host On-Demand for AS/400. Therefore, you cannot run bidirectional OfficeVision/400.

Using installation tips

If the active font control file does not include the Arabic Character Set, download one of the following files from the server to replace the active font control file. These files are located in the /samples/fonts/Bidi directory.

- font.properties.win for Windows
- font.properties.aix for AIX
- f_ar.prp for OS/2

Configuring a workstation

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 AS/400 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

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 and AIX-1046. Select a PC code page first, then select the PC file type.

- For Lam-Alef Expansion, check On.

  Lam-Alef options are valid for only PC Codepage 1256 and AIX-1089.

- For Lam-Alef Compression, check On.

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

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 AS/400

The keys and functions unique to bidirectional Host On-Demand for AS/400 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)

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.

Configuring a workstation

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

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 and AIX 856. Select the PC code page first, then select the PC file type.

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

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
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 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 sessions only.

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)

Understanding VT bidirectional language support (Arabic and Hebrew)

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.

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)

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:

- Backspace (the cursor moves one position to the right)
- Carriage return (the cursor moves to the rightmost position on the current line)
- Line feed (the cursor moves to the rightmost position of the next line)
- 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:

- If the session is configured with one of the 8-bit character sets, that session's 8-bit character set will be loaded.
- 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

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 200 40 500 90	PCs Printers 40 200 90 500

When column heading is on:

Sent by host	Displayed by terminal (RTL screen)
PCs Printers 200 40 500 90	Printers PCs 40 200 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)

Understanding Hindi enablement

Reviewing supported platforms

Hindi sessions run on the Windows 2000 operating system. Select the Indic language group while installing Windows 2000. 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.

Specifying Hindi monospaced font for Windows 2000

Host On-Demand uses Monospaced Devanagari font for a Hindi session on Windows 2000. 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:
   - 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.

   - 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.

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 the behavior of the arrow, Delete and Insert keys

The Insert, Delete, and Backspace keys have some special behaviors in Hindi sessions. This unexpected behavior is because the internal representation of the characters is different compared to what gets displayed on the screen.

Some of the terms used to describe these behaviors include:

Character
The smallest component of written language that has semantic value

Glyph
The shape that characters can have when they are displayed

A single glyph can correspond to a single character or to a number of characters.

Arrows

To move the cursor from one glyph to another on the screen using the left and right arrow keys, you need to press the arrow key more than once for composed characters.

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 three times.

Delete

For certain composed characters, the expected character will not be deleted from the screen when the Delete key is pressed.

Examples

You 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, you expect the Devanagari letter KA to be deleted from the screen. However, the glyph corresponding to Devanagari vowel sign I is deleted from the screen.

In another 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. You reach the glyph Devanagari letter K.SSHA by pressing the right arrow key and when the cursor reaches Devanagari letter K.SSHA, you press the Delete key. Devanagari Letter KA is deleted. But, if you reach the glyph Devanagari letter K.SSHA by pressing the left arrow key and then you press the Delete key when the cursor reaches Devanagari letter K.SSHA, the Devanagari letter SSHA is

deleted.

Insert

For composed characters, the insert function works differently than with standard characters.

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. You reach the glyph Devanagari letter K.SSHA by pressing the right arrow key. If you insert some characters at this position, the inserted characters will be displayed before the glyph Devanagari letter K.SSHA. If you press the right arrow key one more time and then insert some characters, the entered characters are inserted after the first character Devanagari letter KA. The glyph Devanagari letter K.SSHA might disappear, depending on what character you insert.

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 platform.

Thai language support

Understanding supported platforms

For Thai support, you must run the Host On-Demand client on one of the following Thai operating systems:

- Windows 95/98/2000 Thai Edition
  Web browsers: Internet Explorer 4.0 Thai or later, Netscape Communicator 4.06 or later
- Windows NT 4.0 Thai Edition
  Web browsers: Internet Explorer 4.0 Thai or later, Netscape Communicator 4.06 or later
- OS/2 Warp 4.0 Thai
  Web browser: Netscape Communicator 4.04 with JVM 1.1.6 or later. You can download Netscape Communicator for OS/2 and the latest version of JVM at IBM OS/2 Software Choice.
- AIX 4.3 Thai
  Web browser: Netscape Communicator 4.06 or later

Thai sessions can run on non-Thai operating systems (Windows, OS/2 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 some 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.
2. Copy the file to the fonts folder located in the Windows control panel.

Host On-Demand provides the Thai monospaced font Thai Phuket for OS/2 Warp 4.0 Thai and AIX 4.3 Thai Edition.

Configuring Internet Explorer Thai

Microsoft Internet Explorer on Windows Thai Edition does not specify the correct font for Thai. To fix this:

1. Run regedit.exe.
2. Replace Courier with Courier Thai in the following registry entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM\Font Alias\Courier

Configuring Netscape Communicator

If the active font control file (font.properties) in Netscape Communicator (\Program Files\Netscape\Communicator\Program\Java\classes) does not include the Thai character set, do the following:

1. Download font.properties.win from the server.
2. Replace the active font control file (font.properties) with this new font.properties file.

Thai font control file (f_th.prp) is provided for Netscape Communicator for OS/2 Warp 4.0 Thai.

No Thai font control file is provided with Netscape Communicator for AIX 4.3 Thai.

To display Thai on Host On-Demand using a Netscape browser, use Thai raster font (THA3270) for the font name.

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 sesssion.
   - 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

To configure a 3270 printer session, 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. Click the Printer tab.
5. Select the Printer Definition Table (PDT).

   There are three pre-defined Thai PDTs:

- Thai ASCII text mode
- Thai EPSON ESC/P 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.

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 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 AS/400 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

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 keyboard. When an invalid input sequence is entered, Host On-Demand will send 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

Thai is not fully supported on the 5250 ENPTUI function and Database On-Demand.

5250 ENPTUI function

No Thai support on word-wrap function and Continued Entry field.

Database On-Demand

All Thai characters will be converted to question mark symbols (?) when exporting database to 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.