Web-to-Host 6.7

Administrator
Guide

Contents

Product Overview

OnWeb Web-to-Host is a server-based Web application that publishes your existing legacy applications in intranet, extranet, and Internet environments. It includes host display, printer, and file transfer features that enable end users to work productively with host-based information in a familiar Windows or web browser environment. OnWeb Web-to-Host provides access to a broad range of host types, including IBM mainframe, IBM AS/ 400, DIGITAL VAX, UNIX, and HP systems.

System administrators can use the Session Configuration Manager tool to easily configure client sessions that can be published to end users.

Although it can be installed as a standalone product, Web-to-Host is part of Micro Focus Solutions, a common underlying framework that integrates host systems, desktops, browser-based systems, and wireless devices with new Web-based solutions. This guide describes the Web-to-Host standalone version.

For more information on Micro Focus Solutions, visit the Micro Focus web site (*http://www.microfocus.com*).

Components

Web-to-Host includes these components:

*   Pro
*   Java

While both components provide users with display and printer capabilities for mainframe and mid-sized hosts, theyhave different feature sets and use different technologies to connect workstations to host data.

Pro

Designed for use in an intranet environment, the Pro component offers the richest feature set and consists of ActiveX controls that give users access to mission-critical host applications and data. The Pro component provides these client session types:

*   Mainframe Display, Mainframe Printer
*   AS/400 Display, AS/400 Printer, AS/400 File Transfer
*   UNIX Display
*   HP Display

Pro client sessions include these advanced features and options:

*   Mainframe file transfer (can include SimXfer tables)
*   AS/400 File Transfer
*   AS/400 batch file transfers
*   Macros
*   Hotspots
*   User profile enhancements
*   Restricted user support
*   An MSI packaging utility for automatically installing Pro components
*   A distribution utility
*   A download and install service
*   VBA-type scripting

- Customizable Menus and Toolbars
- End-user keyboard mapping
- Administrator keyboard mapping
- Tracing

Hotspots, a word or set of characters on the host screen, activate a function when clicked. Using the **Hotspots Configuration** dialog box, you can enable/ disable, show/hide, create, and modify both default and user-created hotspots. Default hotspots are host commands displayed on-screen. User created hotspots are custom macros you assign to selected on-screen text. You can also use hotspots and macros to log on to and run host applications automatically. Any protected text on your host screen can be turned into a hotspot. In mainframe displays, you can also configure hotspots for non-protected text.

Pro AS/400 File Transfer moves files and data between the host and the PC using either the menu bar or toolbar options of the AS/400 display. A customized toolbar button activates a pre-configured FTX file and starts the AS/400 FTX application. A new AS/400 emulation type has been added to the Session Configuration Manager. It opens the AS/400 FTX application and loads an existing FTX configuration on the client. Your users can customize the file transfer session, configuring options such as the data format for sending and receiving, file locations, application behavior both during and upon completion of the transfer, security settings, and host connection.

With enhanced user profiles, user configuration files (`.cph`) are no longer deleted automatically when changes are made in the HTML files for configurable options. For more information, see *User Profile Configuration*.

Pro ActiveX components are downloaded to the client once, during the first login. A new download service is first installed on the client workstation. Once the service is installed on the client, all users (including restricted users) can work with the Pro ActiveX controls. The service handles all installs, upgrades, and downloads of Pro ActiveX components.

The Web-to-Host Distribution Packager enables you to bundle multiple Web-to-Host configuration and data files into a single, easily distributed package. Users can run sessions that include a complete work environment with components such as pre-defined scripts, macros, hotspots, custom toolbars, background images, icons, screen/font colors, AS/400 File Transfer and Batch File Transfer profiles (for Web-to-Host Pro sessions). The Web-to-Host Distribution Packager helps you provide standardized functionality and a single look and feel for all users. For more information, see the online Help.

Java

The Java component can be used in all environments (Internet, intranet, and extranet), and consists of Java applets (built using JavaBeans) compatible with JDK level 1.6 and higher. The Java component includes these client session types:

- Mainframe Display, Mainframe Printer
- AS/400 Display, AS/400 Printer, AS/400 File Transfer, AS/400 Batch File Transfer
- UNIX Display

Java client sessions include these advanced features and options:

- Mainframe file transfer
- Macros
- Toolbar
- Status bar
- 3D display
- Hotspots
- Color mapping
- End-user keyboard mapping
- A distribution utility

- Administrator-configured keyboard mapping
- Tracing
- Configurable custom options

The Java applets are downloaded to the client once, during the first login; thereafter they operate on the browser system directly with only checks against the Web server for new versions or updates. No other downloads are required until you upgrade the Java component.

Architecture

The figure below shows how Web-to-Host works once the system administrator has created the host sessions and published them to users. The following sections describe how this architecture is applied to each of the component types.
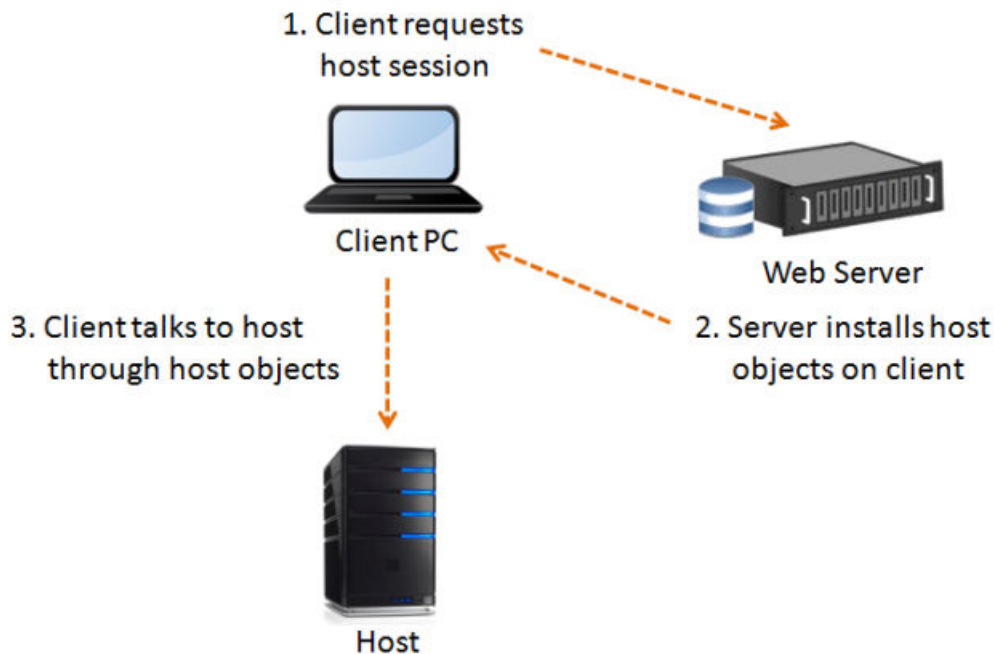
The ActiveX objects and JavaBeans are downloaded to the client the first time a user opens a session. When you install updates on the server, they are downloaded automatically to the client the next time a user opens a session. This architecture enables the client to communicate directly with the host, as shown in the figure above.

Security

Web-to-Host maintains persistent client-to-host sessions. It is important that users be aware of session persistence in relation to information security, especially when sessions are configured to run inside a browser window. In this mode, only one session is visible on the screen at a time, though other sessions could be running in the background.

Users who have access to sensitive information on host systems should consider running each session in a separate window to keep all concurrent sessions visible on the screen. Users can also ensure that all connections are severed by closing their browser when they leave their work area. For details on configuring sessions to run in a separate window, see *Start options*

Web-to-Host supports:

- SSL (Secure Socket Layer) for IBM mainframe, AS/400, and UNIX hosts.
- SSH (Secure Shell) for Pro UNIX display.
- Kerberos authentication for AS/400.

With this security support, users can securely access applications and transfer data between their desktops and mainframe, AS/400, and UNIX systems, encrypting the session data stream to a host capable of supporting these protocols.

Finding information

Web-to-Host product documentation includes:

- This Administrator Guide, which explains how to install, uninstall, configure, and deploy the product.
- The Readme file, which contains information about new features, late-breaking changes, and known issues.

  The **Help** page of the Session Configuration Manager contains links to the Readme file and this Administrator Guide.
- Context-sensitive Help for the Session Configuration Manager, a tool for configuring Pro and Java client sessions.
- User guides for Pro and Java clients. This Help for end users explains how to configure and run features and options in the client session.

Server Installation

To deploy OnWeb Web-to-Host, you must perform the following tasks:

1. Install the product on a Web server.
2. Run the Session Configuration Manager to create and configure (or migrate) session profiles.
3. Publish session profiles to clients.

Web-to-Host files are installed in a `w2hlegacy` directory (created during installation) that must reside in a Web-publishable directory on your server. The Web server can then publish OnWeb Web-to-Host to client machines using HTTP.

System requirements

- The Web server on which you install OnWeb Web-to-Host can be any HTTP based server, such as a Windows Web server, a UNIX server, or an AS/400 (iSeries).
- You must configure this Web server to allow downloads of executable files to the client. If the Web server is a Microsoft Internet Information Server (IIS) or a Microsoft Personal Web server, execute permissions must be turned off for the server directories that contain the Web-to-Host client `.exe` files. See your Web server documentation for instructions.
- You should install OnWeb Web-to-Host software in the root publishing directory of the Web server, or in a subdirectory configured on the web server. Otherwise, the product will not function. For details, consult your Web administrator or your Web server documentation.

  - For Microsoft IIS, this directory is usually:

    `c:\Inetpub\wwwroot`
  - For Apache Server, this directory is usually:

    `c:\Program Files\Apache Group\Apache2.2\htdocs`
- This version of OnWeb Web-to-Host requires Oracle Java VM 1.6 and higher.
- To use the Session Configuration Manager (used to create and migrate client profiles) with either Internet Explorer 6.0 and later or Firefox, Oracle Java VM 1.6 and higher is required.

Installing

This chapter describes how to install and remove OnWeb Web-to-Host as a standalone product on your Web server.

Installing on a Web server running Windows

Using Setup

Follow these steps to install OnWeb Web-to-Host on a Web server running Windows Server 2003 (SP1 and above) or Windows Server 2008.

1. Navigate to the `Micro Focus Web-to-Host 6.7.0\bin` folder.
2. Double-click `Web-to-HostSetup.exe`.
3. Read the introductory information, then click **Next**.

4. Read the Software License Agreement, select the option to accept the terms of the license agreement, then click **Next**.

5. Enter the license key for your OnWeb Web-to-Host product, then click **Validate**.

6. Specify the Web root directory (this can be the root publishing directory of your Web server or any subdirectory under the Web root), then click **OK**.

   • For IIS Web servers, the Web Root Directory defaults to:

      `C:\InetPub\wwwroot\`

   • For Apache Server, the root publishing directory defaults to:

      `C:\Program Files\Apache Software Foundation\Apache2.2\htdocs`

   • For other Web servers, browse to the root publishing directory of the Web server.

   The setup program creates a new `w2hlegacy` directory under the root publishing directory (or the destination directory) and begins copying files to that directory.

   To install to a subdirectory, select **Enable subdirectory support** and type the path in the box provided.

   When finished, the **Installation Complete** screen appears. For an overview of what the correct installation should look like, see *Directory structure*.

7. Click **Finish** to exit the installation.

Using the console

OnWeb Web-to-Host can also be installed using the console (known as console mode). The command line options you enter depend on whether you are installing to the default destination directory or to any other directory configured on the Web server.

If you need to change the license key, you must first uninstall Web-to-Host, then reinstall it with the new key. If you do not enter a license key, Setup installs a 30-day evaluation version.

Installing to the default directory

OnWeb Web-to-Host can also be installed using the console (known as console mode). The command line options you enter depend on whether you are installing to the default destination directory or to any other directory configured on the Web server.

If you need to change the license key, you must first uninstall Web-to-Host, then reinstall it with the new key. If you do not enter a license key, Setup installs a 30-day evaluation version.

To install to the default destination directory:

1. Enter:

   `Web-to-HostSetup.exe -DLicenseKey=<license_key> -i console`

2. Follow the instructions that appear during the installation.

3. When installation is complete, you are prompted for a response. Press `3` to exit the installation.

For example, if the default directory is:

`c:\Inetpub\wwwroot`

then OnWeb Web-to-Host is installed in:

`c:\Inetpub\wwwroot\w2hlegacy`

> **Note:** When you install OnWeb Web-to-Host on either a Microsoft IIS or Apache Server, it is installed to their default directory. Otherwise, it is installed in the `%PROGRAMFILES%` directory as `Web-to-HostSetup.exe`.

Installing to a non-default directory

When installing to a non-default directory, you must enter the Web root directory parameter. If you want to install to a subdirectory under the Web root, you must also enter the subdirectory parameter. However, this is optional.

1. Enter:

   ```
   Web-to-HostSetup.exe -DWebRootDir=<directory_name> -
   DSubDirectory=<subdirectory_name> -DLicenseKey=<license_key> -i console
   ```

2. Follow the instructions that appear during the installation.
3. When installation is complete, you are prompted for a response. Press ENTER to exit the installation.

For example, to install OnWeb Web-to-Host to the following directory:

`c:\InetPub\wwwroot` in subdirectory `w2h6.7\install`

you would enter:

```
Web-to-HostSetup.exe -DWebRootDir=c:\InetPub\wwwroot -
DSubDirectory=w2h6.7\install -DLicenseKey=xxxx-yyyy-vvvv -i console
```

> **Notes:**
>
> - When typing a subdirectory, always use the format:
>
>   `<FolderName>\<FolderName>`
> - Parameters that include a space must be enclosed in quotation marks ("), for example:
>
>   `-DWebRootDir="c:\program files\wwwroot"`

Installing on a Web server running Linux

This version of OnWeb Web-to-Host requires Oracle Java VM 1.6 or higher.

Using Setup

1. Navigate to the `Micro Focus Web-to-Host 6.7.0/bin` folder.
2. Run the `setup.jar` file as a Java executable.
3. Read the introductory information, then click **Next**.
4. Read the Software License Agreement, select the option to accept the terms of the license agreement, then click **Next**.
5. Type the license key for your Web-to-Host product, then click **Next**.
6. Specify the Web Root Directory (this can be the root publishing directory of your Web server or any subdirectory under the web root), then click **OK**.

   For example, the Apache Server root publishing default directory might be one of:

   ```
   /var/www
   /var/www/htdocs
   /var/www/html
   ```

   For other Web servers, browse to the root publishing directory of the Web server.

   The setup program creates a new `w2hlegacy` directory under the root publishing directory (or the destination directory) and begins copying files to that directory.

   To install to a subdirectory, select **Enable subdirectory support** and type the path in the box provided.

   When finished, the **Installation Complete** screen appears.

   For an overview of what the correct installation should look like, see *Directory structure*.

7. Click **Finish** to exit the installation.

Using the console

OnWeb Web-to-Host can also be installed using the console.

If you need to change the license key, you must first uninstall Web-to-Host, then reinstall it with the new key. If you do not enter a license key, Setup installs a 30-day evaluation version.

To install OnWeb Web-to-Host:

1. Change to the directory where `setup.jar` resides.

2. Enter:

```
java -jar setup.jar -DWebRootDir=<directory_name> -
DSubDirectory=<subdirectory_name> -DLicenseKey=<license_key> -i console
```

3. Follow the instructions that appear during the installation.

4. When installation is complete, you are prompted for a response. Press 3 to exit the installation.

For example, to install OnWeb Web-to-Host to the following directory:

`/var/www/htdocs` in subdirectory `w2h6.7/install`

you would enter:

```
java -jar setup.jar -DWebRootDir=/var/www/htdocs -DSubDirectory=w2h6.7/install
-DLicenseKey=xxxx-yyyy-vvvv -i console
```

🖉 **Notes:**

- When typing a subdirectory, always use the format:

  `<FolderName>\<FolderName>`

- The following parameters are optional:

  ```
  -DSubDirectory
  -DLicenseKey
  ```

- Parameters that include a space must be enclosed in quotation marks (").

Installing on an iSeries system

OnWeb Web-to-Host can be installed on any non-Windows server that has a Java run-time environment (JRE) and a Web server.

This section provides instructions for installing Web-to-host on an iSeries system.

System requirements

To support OnWeb Web-to-Host, the following software must be installed on your iSeries system:

- 5722-SS1 Option 12 - Host Servers
- 5722-DG1 - IBM HTTP Server (powered by Apache)
- 5722-JV1 JVM 1.5

Installing the Java Virtual Machine

IBM Technology for Java Virtual Machine is included in licensed program 5722-JV1. Licensed program 5722-JV1 is shipped with the IBM system CDs. To access the **IBM Technology for Java** option, perform the following steps:

1. Enter the Go Licensed Program (GO LICPGM) command, then select **Option 10 (Display)** .

2. If you do not see this licensed program listed, then perform the following steps:

   a. Enter the `GO LICPGM` command on the command line.

   b. Select **Option 11 (Install licensed program)**.

   c. Select **Option 1 (Install)** for licensed program (LP) 5722-JV1 *BASE, then select **Option 8**.

      If **Option 8** is not displayed in the list, you can add it to the list by entering `Option 1 (Install)` in the option field. Enter `5722JV1` in the licensed program field and `Option 8` in the product option field.

3. Add an environment variable. On the command line, enter the following command:

   ```
   ADDENVVAR ENVVAR(JAVA_HOME) VALUE('/QOpenSys/QIBM/ProdData/JavaVM/
   jdk50/32bit')
   ```

Starting Web-to-Host installation

For best performance, use the installation directory specified in this procedure.

1. Using FTP or NetServer, place the `/bin/setup.jar` file from your electronic download in a temporary location on the iSeries. For example, `/tmp`.

2. Enter:

   ```
   QSH
   ```

3. Change to the `/tmp` directory.

4. Enter:

   ```
   java -jar setup.jar -DWebRootDir=<directory_name> -
   DSubDirectory=<subdirectory_name> -DLicenseKey=<license_key> -i console
   ```

   For example, if you were using the APACHEDFT Web server, your command line would look similar to this:

   ```
   java -jar setup.jar -DWebRootDir=/www/apachedft/htdocs -DLicenseKey=XXXXX-
   XXXXXXXXXXX -i console
   ```

5. Follow the instructions that appear during the installation.

6. When installation is complete, you are prompted for a response. Press ENTER to exit the installation.

After installation, you are ready to run the Session Configuration Manager. For information on using the Session Configuration Manager, see *Creating and Migrating Client Profiles*.

Installing on an unsupported non-Windows server

To install the product on an unsupported non-Windows server, you must first install the product on a supported platform (this does not need to be a Web or file server), then copy the files manually to the correct location on the non-Windows Web server.

1. Use FTP to copy the `w2hlegacy` directory and its contents to the root publishing directory of your Web server. For the location of this directory, consult your Web administrator or your Web server documentation).

   🖉 **Note:** When using FTP to transfer files to an IBM OS/390 Web server, be sure to FTP all files with file extensions `.htm`, `.html`, or `.txt` as text. Transfer all other files as binary. This is necessary because IBM uses the EBCDIC rather than the ASCII character set to store text files.

2. When you have copied all the files, the installation is complete. For an overview of what the correct installation should look like, see *Directory structure*.

Installing an evaluation product

This section explains how to install and migrate the OnWeb Web-to-Host evaluation product. The evaluation product expires 30 days after you first install OnWeb Web-to-Host. After 30 days, you can no longer run your session profiles. You should then contact your system administrator.

Installing the evaluation product in graphic mode

To install the evaluation product on your Web server in graphic mode:

1. Follow the appropriate procedure above.
2. Instead of entering the license key, select **Evaluate**.

Installing the evaluation product in console mode

To install the evaluation product on your Web server from the console:

1. Follow the appropriate procedure above.
2. Do not enter the following parameters:

   ```
   -DLicenseKey=<license_key>
   ```

After installing the evaluation product (for all modes), you can create session profiles and begin your 30-day evaluation period by directing your browser to:

<webserver>/w2hlegacy/config/hostwizard.html

For information on creating and configuring profiles, see *Creating and Migrating Client Profiles*.

Upgrading to a licensed product

To upgrade to a licensed product:

1. Install the licensed version on top of your evaluation product. If you are running in console mode, first uninstall Web-to-Host, then reinstall it with the license key.
2. Evaluation profiles expire after the 30-day evaluation period. When upgrading to the licensed product, you must also run all profiles created with the evaluation product through the Conversion Utility in the Session Configuration Manager. See *To migrate profiles after upgrading*.

Directory structure

The installed product has the following directory structure within the *<webroot>*\w2hlegacy\ root publishing directory:

Subdirectory	Description
config\	The configuration utility, hostwizard.html.
data\	The sub-directories into which keyboard maps, scripts, macros, distribution packages, AS/400 FTX configuration, and watermark files are copied for all clients.
help\	The online documentation (Help) files.
images\	The graphics used by OnWeb Web-to-Host.
java\	The download software for Java client connections.
javascript\	The include files used for some JavaScript functions.

Subdirectory	Description
`pro\`	The download software for Pro client connections.
`rss\`	The software for secure connections.
`utils\`	The Java Uninstall utility, MSI Packager, OnWeb Demo Server utility, and other useful utilities.

Note: If you choose to place the user data files location outside the OnWeb Web-to-Host server installation folder, you must copy the file `web.config` from `w2hlegacy` to the new location. This is because the `web.config` file contains declarations of the MIME types to be allowed by IIS7.

Session Configuration Manager

After installing OnWeb Web-to-Host on your Web server, the next task is to use the Session Configuration Manager to create, edit, and migrate client profiles. To run the Session Configuration Manager, direct your browser to the following URL:

`<webserver>/<destination directory>/w2hlegacy/config/hostwizard.html`

For information on using the Session Configuration Manager, see *Creating and Migrating Client Profiles*.

Troubleshooting

This section summarizes the most common problems encountered when installing Web-to-Host.

Session Configuration Manager is lost

If after installing the product you cannot find the Session Configuration Manager, you may have installed the product to the wrong directory. If the product is correctly installed and you still cannot find the Session Configuration Manager, then search for the file `hostwizard.html` in the root publishing directory. When you find it, note the URL for the Session Configuration Manager for future use.

Web server: Session Configuration Manager does not open

If you correctly installed the product and still cannot open the Session Configuration Manager in your browser, you may have a case-sensitive file system. Verify that all the directories and file names for OnWeb Web-to- Host are in lowercase, enter the URL in lowercase, and try opening it again.

If you changed the product directory names from the default structure described in *Directory structure*, the `<OBJECT>` tag's codebase property is incorrect and must be fixed in the HTPL files:

1. First, back up the HTPL files in the `config\` directory.
2. Open each file with a text editor (such as Notepad) and edit the directory names.
3. Save each file as ASCII text.

Uninstalling

When removing OnWeb Web-to-Host from your network environment, you should also uninstall the product from all client machines. For details on this procedure, see *Client uninstall*.

Uninstalling from a Windows server

1. Select **Control Panel** > **Add/Remove Programs**.
2. Select **Micro Focus OnWeb Web-to-Host 6.7**, then click **Add/Remove**.
3. Follow the prompts to remove the application.

Uninstalling from a non-Windows server

To uninstall from the default destination directory:

1. Navigate to:

   `<default_install_directory>\w2hlegacyuninst`
2. Enter:

   `java -jar uninstaller.jar -i console`

To uninstall from any destination directory and subdirectory:

1. Navigate to:

   `<webroot_directory>/<subdirectory>/w2hlegacyuninst`
2. Enter:

   `java -jar uninstaller.jar -i console`

Uninstalling from the default installation directory

To uninstall from the default installation directory:

1. Navigate to:

   `<default_install_directory>\w2hlegacyuninst`
2. Enter:

   `java -jar uninstaller.jar -i console`

Uninstalling from a non-default installation directory

To uninstall from a non-default installation directory:

1. Navigate to:

   `<webroot_directory>/<subdirectory>/w2hlegacyuninst`
2. Enter:

   `java -jar uninstaller.jar -i console`

Creating and Migrating Client Profiles

After installing OnWeb Web-to-Host on your Web server, the next task is to create or migrate client profiles. You may also want to edit client profiles to configure new options, such as security, distribution packages, Pro toolbars and menus, and Pro watermarks.

This chapter explains how to use the Session Configuration Manager to create, edit, and migrate client profiles and how to deploy client profiles to your users. The procedures in this chapter apply to a standalone Web-to-host installation on any Web server.

> **Note:** On a slow connection, the initial download for the Session Configuration Manager and the client session may take some time. Consequently, Web-to-Host may seem as though it is not responding when running the Session Configuration Manager or the client session for the first time.

Migrating client profiles from a previous version

After updating Web-to-Host product by installing a new version or upgrade, you must migrate all session profiles created in the previous version by running the Session Configuration Manager in server mode. If you do not update the session profiles, the following problems may occur:

- Pro client sessions will not open. Users will see an error message prompting them to contact their system administrator.
- Java client sessions will not open and users will not see an error message.

For details on running the Session Configuration Manager in server mode, see *Creating client profiles*.

Migrating profiles after upgrading

1. Run the Session Configuration Manager on the server by typing the following in the address bar of your browser:

   ```
   http://<webserver_name>/<subdirectory>/w2hlegacy/config/hostwizard.html
   ```

2. Do one of the following:

   - To quickly migrate profiles in batch mode, click the **Conversion Utility** tab, then follow the *Running the conversion utility* procedure below.
   - To convert and edit profiles individually, click **Open an Existing Session or Import PC-to-Host Profile**, then specify the profile to edit. When prompted to convert the profile prior to editing, click **OK**. For details on editing profiles, see *Creating client profiles*.

   Both migration methods ensure that your Web-to-Host installation incorporates the most recent version numbers in the session HTML files. Once new software is downloaded to the client workstations, the version numbers on client workstations and session files must match. If new parameters exist in the current product version that were not defined in the migrated profile, Web-to-Host uses the default values.

3. When the user opens a migrated profile, the browser displays a standard security dialog box asking if the user wants to install and run software from Micro Focus.

   Administrators should tell their users to click **Yes** (for Internet Explorer) or **Grant** (for Firefox).

Running the Conversion Utility

1. If necessary, run the Session Configuration Manager in server mode, then click the **Conversion Utility** tab. For details, see Steps 1 and 2 in the procedure above

2. In the **Current Directory** box, type the drive and full path of the folder containing the session profiles to convert.

- To change directories, in the **Directories** box, double-click either the double dot [**..**] or the directory names until you are at the desired directory.
- To change drives, in the **Current Directory** box, type the drive letter followed by a colon (for example, D:), then press ENTER.

3. In the **Files** box, select the files to convert. You can select one or more files and convert them simultaneously.

4. Click **Convert**.

   The **Results** box shows the status of the requested conversion(s) by denoting Successful or Failed next to the file name(s).

   - If the conversion is successful, the file is updated and the previous version is saved in the same directory with a .bak extension.
   - If the conversion failed, your browser's Java Console output screen (found on the Internet Explorer **View** menu or on the Firefox **Window** menu) contains an error message explaining why the conversion failed.

5. To exit the Conversion Utility, close the browser.

Migrating Rumba PC-to-Host profiles

Moving from Rumba PC-to-Host to Web-to-Host does not mean you lose profiles or that those profiles must be recreated. Web-to-Host provides a migration wizard that makes upgrading fast and easy and allows you to continue using your old profiles. The migration wizard is part of the Session Configuration Manager.

Supported PC-to-Host profiles

The migration wizard converts the following PC-to-Host profiles:

Rumba Client	File Extension
Mainframe Display	.WDM
Mainframe Printer	.WPM
AS/400 Display	.WDA
AS/400 Printer	.WPA
AS/400 File Transfer	.RTO
AS/400 Batch Transfer	.BTF
UNIX Display	.WDU
HP Display	.WDH

During the migration process, all relevant parameters are converted to either Java or Pro sessions and placed in the Session Configuration Manager.

Note: It is recommended that you migrate profiles on the computer where Rumba PC-to-Host is installed. If you want to make the profiles available for other clients, you must manually copy the data files, keyboard maps, macros, and scripts to the Web-to-Host server.

Importing profiles using the Session Configuration Manager

1. Open the Session Configuration Manager utility in server mode.
2. Click the **Create** or **Edit Session** tab.
3. Select **Open an Existing Session** or **Import PC-to-Host Profile** , then either enter the full path or click **Browse** to select the path of the file to import. When the file is imported, the **Type** option (which displays the type of profile type imported) in the **Create New Session** box is dimmed, and the **Implementation** option is available.
4. From the **Implementation** drop-down list, select the client appropriate for the particular profile. For example, Java client or Pro Client.
5. Click **Go**. When the migration process is complete, the Session Configuration Manager opens with the imported data displayed in the relevant option boxes. For example, the IP address that was in the Rumba PC-to-Host profile now appears in the IP address box of the Session Configuration Manager. If Web-to-Host requires a parameter not found in the imported profile, it uses the default value and displays a Migration Notification listing the parameters not found.
6. Once the profiles have been imported, assign a session name, then save and continue editing as you would with any Web-to-Host profile.

Creating client profiles

This section describes how to use the Session Configuration Manager to create a new Web-to-Host client session for your users. The Session Configuration Manager utility saves your client configuration settings in an HTML file that invokes a named Web-to-Host client session.

The standard method in which the system administrator creates and configures the session profiles is known as server mode. In this mode, the profiles must reside in a Web-published folder on the Web-to-Host server. When the user opens a profile on the server, the client session is delivered to the desktop through the browser.

To run the Session Configuration Manager, type the following in the address bar of your browser:

```
http://<webserver_name>/
```

```
<subdirectory>/w2hlegacy/config/hostwizard.html
```

Creating or editing a client profile

To use the Session Configuration Manager to create or edit client profiles:

1. Run the Session Configuration Manager on the server or on your local workstation.
2. Optional: For general instructions on using the Session Configuration Manager, click the **Help** tab. This tab also contains links to the Readme file and this Administrator Guide.
3. Click the **Create** or **Edit Session** tab, then do one of the following as needed:

   - Create a new session. Click **Create a New Session**, then select the **Type** (host emulation session type) and **Implementation** (Pro or Java client).
   - Edit an existing session. Click **Open an Existing Session**, then specify the full path of the HTML session configuration file to edit. The **Browse** utility defaults to the location of the last saved configuration file.
4. Click **Go!**.

   The tabs for the selected host type and technology implementation appear.
5. Optional: Click each tab, click **?** at the bottom of the screen, then print the help pages for each tab.

6. Configure the settings on each page as needed.

- For details on each field, see the online help. For details on configuring client start options, concurrent sessions, and multiple language support, see *Configuring client profiles*.
- The Session Configuration Manager displays an exclamation mark next to required settings, and provides many default settings. You need to enter only a few unique settings to make your connections work correctly. However, you should check each page to be sure you select the appropriate options for your needs.

7. To save the profile, click the check mark icon at the bottom of the Session Configuration Manager.

   Web-to-Host generates the HTML file and displays the **Save As** dialog box.

8. Specify an appropriate folder in which to save the profile.

   In server mode, you must save the profile in a Web-published folder. Otherwise, client sessions do not receive automatic updates from the Web server.

   Note: In previous versions of Web-to-Host, updates from the administrator deleted all user configurations. In this version, there are cases when administrator changes do not automatically delete the user's configuration (`.cph`) file. For more information, see *User Profile Configuration*.

Configuring client profiles

This section describes some of the common options you can configure when creating or editing client profiles in the Session Configuration Manager. For a list of options related to each technology, see the Session Configuration Manager Help .

Start options

The following options are located on the **Session Options** page when creating or editing client profiles in the Session Configuration Manager:

Run in a Separate Window

> This option applies only to Pro and Java display profiles.
>
> The **Run in a Separate Window** option opens the client session in a separate browser window.
>
> You can also use this option to configure a Pro display profile to launch multiple standalone sessions using the same configured connection. For details, see *Multiple sessions*.
>
> The default is **Clear**. The host session runs inside the browser.

Server URL

> With this option, you have the ability to run sessions from a web server other than the default Web-to-Host server. The URL you enter indicates the location of the alternate Web-to-Host server.

Enable Local Start

> This option applies only to client profiles created by running the Session Configuration Manager in server mode. For information on server mode, see *Creating client profiles*.
>
> The **Enable Local Start** option allows users to run host sessions when the web server is unavailable. With this option, whenever the user opens a client profile stored on the web server, Web-to-Host copies that profile to the client workstation. The profile resides on the web server as an HTML file that is named after the client session. The profile location on the client workstation varies, depending on the client type and the browser:

- Pro sessions:

  ```
  %LOCALAPPDATA%\Micro Focus\Rumba\LocalStart
  ```
- Java sessions:

  ```
  %LOCALAPPDATA%\Micro Focus\Rumba\JavaLocalStart
  ```

It is best to run client profiles from the server to ensure that users have the most up-to-date configuration and software.

When running Local Start profiles, help files are only available if, during configuration, the administrator selected **Install User Guide locally**. Auto macro files and keyboard map files configured by the administrator are cached on the client workstation when the session is downloaded from the server, so these local copies are accessible to the client session when the originating server is down. By default, Local Start is not selected.

Multiple sessions

Users can run concurrent Web-to-Host sessions and switch between session windows to perform tasks. How users initiate multiple sessions and navigate between them depends on how you configure the session profiles. There are three scenarios:

- Multiple sessions running in separate browser windows

  By default, users must open multiple instances of the browser to start multiple client sessions. Users can run concurrent host sessions and switch between sessions by clicking each browser window in turn.
- Multiple sessions running outside the browser

  Administrators can configure Pro and Java display profiles to run in a separate window outside the browser (see *Start options*). The user must open a new instance of the browser to launch another host connection but, once the new session is connected to the host, the browser can be closed without losing the connection.
- Multiple Pro standalone sessions

  Administrators can configure a Pro display profile to launch multiple standalone sessions using the same configured connection. For example, a user can run two or more MyRumbaHost sessions, each in its own window.

  With this configuration, a new session opens in a separate window outside the browser whenever the user accesses a session URL through the browser window. After launching one or more session windows, users can close the browser without losing the host connection.

Configuring multiple Pro standalone sessions:

1. Create or edit or the Pro session profile in the Session Configuration Manager, then click the **Session Options** tab.
2. Check **Run in a Separate Window** and **Allow Multiple Standalone Sessions**.
3. To save this configuration, click the check mark icon at the bottom of the page.

When you enable these two options, users can launch a new session window using any method that requests the session URL. For example, if your Web site includes a Pro display session called `Display.html`, users can open multiple sessions by:

- **Clicking a link on a Web page**

  If the Web page includes a link to `http://<yoursite>/Display.html`, users can click this link to launch a new session window.
- **Refreshing the browser with the session URL listed in the address bar**

  When the browser's address bar contains the session URL, users can click the **Refresh** (or **Reload**) button on the browser toolbar to launch a new session.

- **Typing the address in the address bar**

  If users have browsed to another location after opening the session, they can enter the session URL in the address bar to launch another session window.
- **Recalling the address from history**

  If users cannot remember the URL, they can open the browser's history list and then select the session URL to launch a new session window.

Users can switch between sessions by clicking each of the windows in turn, or by using the taskbar. If the browser closes, the session windows remain open.

International client sessions

When using the Session Configuration Manager to create or edit client profiles, configure the following multi-lingual options to meet the language needs of your users:

You can set these options to use different languages if necessary. For example, you can set the user interface to English and set the keyboard map and host character set to German.

Host Character Set

This option sets the host language (also known as the codepage). When configuring Pro and Java AS/400 and mainframe display or printer profiles, the option appears on the **Connection** page.

To specify the **Host Character Set**, select the language character set (or codepage) for the client session. If the host uses a non-English (United States) language, select the language used by the host.

The host character set includes commonly used marks, accents, letters, and symbols of a specific language. For example, if the host language is French, the host character set must also be French to ensure that French special characters are transmitted to the host correctly and that the characters received from the host display in the client session correctly.

The default setting is English (United States) - 37.

UNIX character set options
National Replacement Character Set

> Replaces particular ASCII characters with characters of the specified language.

Supplemental Character Set

> Specifies the character set used by the host.

When configuring a Pro UNIX display, these options are located on the **Client Options 2** page.

When configuring a Java UNIX display, these options are located on the **Character Set Options** page.

> **Note:** There are no configurable character set options for HP display sessions.

Keyboard mapping options

These options set the country or custom keyboard map for Pro and Java display sessions.

Web-to-Host supplies numerous country keyboard maps to accommodate the special characters and symbols used in various languages. You can deploy country keyboard maps in several ways. For example, you can:

- Standardize all the sessions on one country keyboard.
- Base the keyboard map on the client workstation's regional settings.
- Enable the user to specify their own keyboard mappings.

When configuring display profiles, the available keyboard mapping options vary, depending on the session profile type.

Pro display clients

When using the Session Configuration Manager to configure Pro AS/400, mainframe, UNIX, and HP display profiles, thee following options appear on the **Keyboard Map** and **Auto Macro** pages:

Keyboard Map

You can select a standard country keyboard map or specify a custom keyboard map (`.map` file) for the client session. For information on how to do this, see the Help. The default keyboard map is **U.S.A.**

Custom Keyboard Map

The default is blank.

> **Note:** To enable users to specify their own Pro keyboard map files, which override the administrator-specified keyboard map, see the Session Configuration Manager Help on the **Client Options** page when configuring Pro display profiles.

Java display clients

When using the Session Configuration Manager to configure Java AS/400 and mainframe display profiles, the following options appear on the **Keyboard Map** and **Auto Macro** pages:

Custom Keyboard Map

The default **Custom Keyboard Map** value is blank, and the client session uses a standard country keyboard map based on the keyboard Locale. For details on specifying a custom keyboard map (`.map` file), see the online help for the appropriate page in the Session Configuration Manager.

Keyboard Locale

The keyboard locale determines some default keyboard mappings for the client session. The default value uses a standard country keyboard map based on the **Client Locale** setting.

When configuring Java UNIX display profiles, these options appear on the **Keyboard Options** page.

> **Note:** To enable users to specify their own Java keyboard mappings, which override the administrator-specified keyboard map, see the Session Configuration Manager Help on the **Client Options** page for Java AS/400 display or Java mainframe display profiles or the **Tool Options** page for Java UNIX display profiles.

Client Locale

This option sets the language of the Web-to-Host client user interface for display and printer sessions.

When using the Session Configuration Manager to create or edit any profile (except Java UNIX profiles), this option appears on the **Client Options** page. For Java UNIX profiles, this option appears on the **General Display Options** page.

For Pro and Java sessions, the Client Locale specifies the language for the Web-to-Host client user interface, which consists of the session window (including tool tips and the status bar), dialog and message boxes, error messages, and Help.

The default value is English.

Multiple language scenarios

When running client sessions, users may need to view applications on an international host, require a different country keyboard map, or require the Web-to-Host client user interface in another language. This can be done by configuring the **Host Character Set**, **Keyboard Mapping**, and **Client Locale** options.

Different companies have different international language environments and require different display and/or printer configurations. As such, it is impossible to provide a single procedure. This section lists possible multi-language scenarios to help you determine how to best configure the options for your international language environment.

In the following table, the first column lists the multi-lingual option, the second lists language scenarios, and the third lists the suggested Web-to-Host settings.

Note: There are multiple keyboard listings because Web-to-Host provides several keyboard mapping options. For information on individual settings, see the Help associated with the page in the Session Configuration Manager.

Option	If	Then
Host language	The host uses a language (codepage) other than English (United States).	In the **Host Character Set** option, select the language of the host.
Keyboard	All clients are localized on one language.	**Pro:** In the **Keyboard Map** option, select the country keyboard map or specify the full path of the **Custom Keyboard Map** file.
		Java: Specify the **Custom Keyboard Map** file name or select the **Keyboard Locale**.
	Clients are localized on different languages as indicated by different regional settings (**Control** page) on the client workstations.	**Pro:** Select **Use Client Regional Settings** from the **Keyboard Map** option
		Java: Specify a blank **Custom Keyboard Map** option (default) and **<Default>**.
		Keyboard Locale (default).
		Each client uses the keyboard map based on its regional settings.
	Users need or want control over their own keyboard maps.	**Pro and Java:** Enable end-user keyboard mapping. User-created keyboard maps override any country keyboard map specified in the **Keyboard Map** option.
Client user interface	The client user interface uses a language other than English and you want Web-to-Host to use the same language.	Select the appropriate language from the **Client Locale** option.
		Note: Web-to-Host supports English, French, and German.

The following are some other multi-language environments and suggested configurations:

- Clients connect to a host using the German language (codepage) and their regional settings are set to German. In this scenario, you would set the client host character set, country keyboard map, and client user interface language to German.
- Clients connect to a host using the English (United States) language (codepage), but their regional settings are set to French (Canadian). In this scenario, you would set the client host character set to English (United States), but the country keyboard map and client user interface language to French (Canadian).

- Clients connect to a host using the English (United States) language (codepage), but some client regional settings are set to French (Canadian) and others to German. In this scenario, you would want to set the client host character set to English (United States), deploy a country keyboard map based on the client regional settings, and set the language of the client user interface to either French or German.
- Clients connect to a host using the Spanish language (codepage) and their localization settings are set to Spanish. In this scenario, you would set the Web-to-Host host character set and the country keyboard map to Spanish. However, because Web-to-Host does not provide a Spanish client user interface, the client user interface language must be set to English, French, or German.

Java Web Start

Oracle Java Web Start Application Manager can now be used to manage Java sessions created in Web-to-Host. Java Web Start enables users to be browser independent by running sessions in their own, separate window. Users can also choose to run Java Web Start sessions via a standard browser. With Java Web Start Application Manager, users can add and remove sessions from their workstation and create desktop shortcuts for quick access to individual host sessions.

When a session is run for the first time using Java Web Start, all files required to run the session are automatically downloaded and installed on the client workstation. After this, the application checks the server-side session (JNLP) file and Java applet version. Updated files are downloaded automatically when needed. If the server is unavailable when the check is performed, the session is run with the existing configuration.

Requirements

To run Java sessions with Java Web Start, you need the Java Runtime Environment (JRE) 1.6 or higher.

If you want to run Java Web Start sessions through a standard browser, the Web server to which you published the Web Start sessions must recognize the `.JNLP` extension and MIME type, `application/x-java-jnlp-file`. If the server does not already recognize this type of file, you must add it manually.

Adding MIME types

For Apache servers:

1. From `Program Files`, browse to the `Apache\conf` folder.
2. Open the `mime.types` file in a text editor.
3. Add `application/x-java-jnlp-file` under `MIME Type`.
4. Add `JNLP` under `Extension`.

For Windows 2003 servers with IIS 6 and for Windows 2008 Server with IIS7, this is done automatically by the Web-to-Host installer.

When `hostwizard.html` is being opened, the following error may occur:

```
Cannot add duplicate collection entry of type 'mimeMap' with unique key
attribute 'fileExtension' set to '.abc'
```

If this happens, the following line should be removed from the `web.config` file:

```
<mimeMap fileExtension=".abc" mimeType="xyz/uvw" />
```

Creating sessions for Java Web Start deployment

You can create Java Web Start sessions from scratch or from Web-to-Host HTML sessions. The reverse also applies if you want to create an HTML Web-to-Host session from a Java Web Start session.

1. Create or edit a Java session in the Session Configuration Manager.
2. On the **Session Options** page, select **Enable Java Web Start (Oracle JVM only)**. (Clear the check box to create an HTML Web-to-Host session.)

3. In the **URL folder** box, enter the URL where you want to publish the session. (If you unchecked the box, this option is unavailable.)

4. Save the session.

✎ **Note:** Java Web Start sessions should only be saved on a Web server. In addition, the full, legal URL path to the location where you published the sessions must be entered in the Session Configuration Manager. Some sessions will not function properly. These are those created using the localhost address, containing workstation names, or using an address obtained while browsing to the file, for example with Windows Explorer. Sessions can be saved, however, to any Web server, even those that do not have Web-to-Host installed.

When a Java Web Start session runs, the `.JNLP` file and associated applets are updated from the server. However, the session itself runs locally from the client workstation. Sessions run locally do not have access to online Help files unless you select the **Install user guide locally** option when creating the session.

Defining password level caching policy

Password level caching is involved with the AS/400 display or AS/400 file transfer.

On AS/400 hosts, password protection capabilities can be set to different levels, such as short or long passwords. Client applications connecting to a AS/400 host must first query the password level set on the host. This slows down overall system performance, increasing both connection time and network traffic.

To save time, Web-to-Host caches password-level data, by default. The first time the password level is queried, the data is saved on the client PC. Afterwards, to avoid performance degradation, the cached password level value is used for each connection.

Cached data is host specific. Once the password level has been cached for a particular host, it is used by all sessions connecting to that host.

The following changes should be performed on the Java Script parts of the HTML session configuration files:

AS/400 Printer Pro Client

Comment out the old `HostPwdLevel` property setting.

AS/400 Display Pro Client

Comment out the old `HostPwdLevel` property setting.

Add the `this.ResolvePwdLevelPolicy` property setting to the `stAS400DisplayProps()` function:

Property setting	Description
`this.ResolvePwdLevelPolicy = 0`	Query and cache the password level value once and use it from now on. Default value.
`this.ResolvePwdLevelPolicy = 1`	Always query and cache the password level value on each connection.
`this.ResolvePwdLevelPolicy = 2`	Never query the host for the password level value and use the lowest password level value on each connection.

Example:

```
function stAS400DisplayProps()
{
        this.SetMinFontSize = false;
        this.FontPointSize = 0;
        this.TypeAhead = true;
        this.AutoReset = false;
```

```
        this.StartupModelType = 2;
        // HostPwdLevel is now deprecated. It should be cleared from old
sessions.
        //this.HostPwdLevel = false;
        this.SuppressDialogs = false;
        this.ResolvePwdLevelPolicy = 2;      // (0=Once, 1=Always, 2=Never)
}
```

Publishing client profiles to users

You can use any usual Web publishing method to publish session profiles created by running the Session Configuration Manager in server mode to users. For example, you can:

- Provide the URLs of the session profiles for users to enter in the address bar of their browsers.
- Create an HTML page containing links to the sessions and organize these links by host type or other useful groupings.

OnWeb Client Installation

This chapter describes procedures that users must follow when installing, updating, or removing OnWeb Web-to-Host files on the client workstation. If Rumba PC-to-Host software is installed on the client workstation, users should follow the procedures described in *Coexistence: Pro and PC-to-Host* instead, to ensure successful coexistence with Web-to-Host.

System requirements

This section describes the minimum system requirements and configurations required for client workstations to run Web-to-Host components.

Client operating system

Web-to-Host supports these client operating systems:

- Windows 7 and 8
- Windows Vista
- Windows XP
- Windows 2003

Microsoft Windows Installer (MSI), an installation and configuration service, must also be installed on the client PC before installing Web-to-Host Pro and advanced features of Java, such as native access.

If no MSI is on the client workstation, an error message is displayed. Web-to-Host does not pre-install MSI. You can download the latest version from:

http://www.microsoft.com/msdownload/platformsdk/sdkupdate/psdkredist.htm

Client JRE

Web-to-Host Java components have been tested with the following JRE families:

JRE Family Version	Full Version
8	1.8.0_5
7	1.7.0_65
6	1.6.0_30

Client browser

Web-to-Host supports these browsers:

- Internet Explorer
  - 32-bit version of Internet Explorer 6.0 or later (for Pro components) with these features enabled:
    - ActiveX and VB Script
    - JavaScript
  - Both 32-bit and 64-bit versions of Internet Explorer 6.0 or later (for Java components) with these features enabled:
    - VB Script

- JavaScript
- Firefox (for Java components only) with these features enabled:
  - Plug-ins
  - Java and JavaScript
  - Smart Update
- Chrome (for Java components only) with these features enabled:
  - Plug-ins
  - Java and JavaScript

Host requirements

Java AS/400 File Transfer clients require the following AS/400 host software:

- Clients without SSL require OS/400 version V4R3 or later
- Clients with SSL require OS/400 version V4R4 or later

Client install and upgrade

This section describes how users install and update Web-to-Host when the client does not have Rumba desktop software also installed. Users must follow these procedures the first time they open a Web-to-Host session, and repeat these procedures each time Web-to-Host is updated.

When the user starts a Java session, the browser automatically verifies whether current Web-to-Host files are installed for all host types. Installation procedures are specific to the client browser type. Pro sessions are installed through the Service Manager.

Installing Pro

Web-to-Host Pro components can be installed automatically using either the MSI Packager or the Service Manager.

The Web-to-Host MSI Packager is a utility for Pro Clients that replaces CD Image Creator and `SetProInstallPath.exe`. When integrated with the Service Manage, the MSI Packager provides complete local start capabilities. You create custom installations that can be deployed on restricted-user systems. You can add all of the Pro emulation types, SimXfer tables for AS/400 file transfer, RSS Client security, a VBA-type script engine, localized client Help, and distribution packages. For more information on MSI Packager, see the online *MSI Packager User Guide* supplied with the product.

Service Manager is installed on client workstations by a user with administrator rights. Once the Service Manager has been installed, it downloads and installs all Pro components regardless of user rights. The rest of this section describes installation using this component. By default, all Pro files are installed in:

`C:\Program Files\Micro Focus\Rumba`

> **Note:** Web-to-Host Pro is compatible with Rumba PC-to-Host version 9.3 only. All other Web-to-Host components work with all versions of Rumba PC-to-Host. For details on co-existence restrictions for the Pro component and Rumba PC-to-Host , see *Coexistence: Pro and PC-to-Host*.

Standard install procedure: Pro

1. From the browser, run the session HTML created by the Session Configuration Manager. As Web-to-Host downloads and installs, a progress dialog is displayed.
2. Depending on your browser security settings, the **Security Warning** dialog box may appear asking if you want to install the Service Manager. Click **Yes** to run the install. Once the Service Manager is installed, all necessary Pro ActiveX controls are installed and the session opens.

Note: There may be instances where a message appears in the browser window telling you to restart the computer. If it appears, click **OK**. After restarting, open Internet Explorer, click the extension you want to connect to, then proceed with your host session.

Silent Install procedure: Pro

As mentioned above, the standard Web-to-Host Pro installation displays a progress dialog while downloading and installing. However, it is possible to run a silent installation. That is, an install and download with no progress dialog displayed. To do this:

1. Navigate to `\w2hlegacy\config\productcfg.xml`. This file contains component descriptions and version numbers.
2. In the `<product_info>` section, change the `silent_install` property to `true`. By default it is set to `false`. After editing, `silent_install` should be:

   `<silent_install value="true"/>`.
3. After making the necessary change to `productcfg.xml`, follow the standard installation procedure.

Installing Java

The Web-to-Host Java component can be installed automatically on Internet Explorer, Firefox, and Chrome clients. The installation procedure is the same for all browsers.

To install the Web-to-Host Java component:

1. From your browser, log on to the Web server and click a session name to request a host session.
2. Depending on your browser security settings, the **Security Warning** dialog box may appear. Click **Yes** to run the install. Your host session starts.

Note: Restricted users cannot install the Web-to-Host Java component. However, once an administrator installs the Web-to-Host Java component, restricted users can run a Java session. Local help components must be installed by an administrator before they can be used by restricted users.

Client uninstall

You may occasionally need to uninstall Web-to-Host components and reinstall them to reload lost files and correct other system problems. File and directory names and locations to which Web-to-Host components are installed vary by component, browser type, and version. As a result, the procedures for uninstalling Web-to-Host components are specific to each context, as described in the following sections.

Uninstalling Pro

Before uninstalling you must first close any open windows. Use the following procedure to uninstall the Pro component.

1. From Windows Control Panel, double-click **Add/Remove Programs**. The **Add/Remove Programs Properties** dialog box appears.
2. From the **Install/Uninstall** tab, select **Micro Focus OnWeb Web-to-Host Pro Client 6.7.0**, then click **Add/Remove**.
3. From the **Web-to-Host Pro Client Uninstall** message box, click **OK** (to continue uninstalling the program). The program uninstalls and you return to the **Add/Remove Programs Properties** dialog box.
4. Click **OK**.

Note: You must delete one file manually.

1. Open `c:\Windows\Downloaded Program Files\`.
2. Right-click **Pro Client Persistent Session Control** and select **Delete**.
3. Click **Yes** to delete the file.

Uninstalling Java

To uninstall Java Session, from the **Java Control Panel**, clear **Temporary Internet Files**.

Uninstalling the Session Configuration Manager

When you run the Session Configuration Manager, the tool is installed locally if you are using Internet Explorer, but is run from the cache if you are using Firefox or Chrome.

To uninstall the Session Configuration Manager, from the **Java Control Panel**, clear **Temporary Internet Files**.

Coexistence: Pro and Rumba PC-to-Host

Rumba PC-to-Host, a traditional desktop PC-to-Host application that runs on Microsoft Windows 7 and 8, Vista, XP and 2003 clients, and OnWeb Web-to-Host Pro have shared executable files. Consequently, certain conditions must be met for both products to coexist on the same client workstation.

Web-to-Host Pro 6.7 is completely compatible with Rumba PC-to-Host 9.3. In most cases, there should be no problems when applying feature TMPs to Web-to-Host Pro and Rumba PC-to-Host.

> **Note:** The Web-to-Host Java components are compatible with all versions of Rumba PC-to-Host products.

By default, the Web-to-Host Pro installation writes all program files on the client workstation to:

```
C:\Program Files\Micro Focus\Rumba
```

User data files are written to locations that vary depending on the user's environment. For details, see *User Data File Locations*.

Coexistence requirements

The client workstation must meet these requirements for the Web-to-Host Pro component to coexist with Rumba PC-to-Host:

- The Rumba PC-to-Host product version must be version 9.3. The Pro software is currently not compatible with earlier versions.
- You must install both products in the same language.
- If an incompatible Rumba PC-to-Host product is installed, you must remove it before installing the Web-to-Host Pro controls.

To determine the way Pro deals with different coexistence conditions, edit the following parameters in the `w2hservercfg.xml` file, located in the `config` folder on the Web-to-Host server.

- `CoExistProblemBehavior value="0 |1"`.

  A value of 0 means that, when an incompatible version of PC-to-Host is encountered, a message appears stating that the version is incompatible and that installation of Web-to-Host Pro has stopped. A value of `1` automatically uninstalls the incompatible version without notifying the user.

- `CoExistProblemMessage value=<message>`.

  A default message informs the user that an incompatible version has been detected. However, you can customize the message. This is useful if you want to include extra information. For example, help desk contact information or the path to a compatible version of Rumba PC-to-Host. Changes you make to the `w2hservercfg.xml` file apply to all user sessions connecting to the server. User created files, such as macros and keyboard mappings, are not deleted when the incompatible version is uninstalled.

Setting a custom install path

As mentioned previously, Web-to-Host Pro installation places all program files on the client workstation, by default, in:

```
C:\Program Files\Micro Focus\Rumba
```

By default, Rumba PC-to-Host also places its program files in the same location. If Rumba PC-to-Host is installed first, Web-to-Host Pro installs its program files to the same location and both products coexist.

However, if Web-to-Host Pro is installed first, the destination path in the Rumba PC-to-Host install wizard is dimmed and cannot be changed.

To install Web-to-Host Pro first to a customized location, use the MSI Packager tool located in `\utils \MSIPackager`. For more information on MSI Packager, see the Help supplied with the tool.

Upgrading Pro and PC-to-Host software

When you install a new Web-to-Host version or Service Pack, the new Pro software automatically downloads to the client workstation when the user opens a Pro session. A start-up program compares the Pro and Rumba PC-to-Host desktop versions. If the versions are not compatible, the user receives a message determined by the option configured in the `w2hservercfg.xml` file.

User Profile Configuration

There are two types of Pro configuration settings in Web-to-Host:

- Administrator settings - created by Web-to-Host administrators using the Session Configuration Manager and deployed to the users as HTML session files.
- User settings - stored in a local configuration file (`.cph`). If the administrator has enabled editing specific options in the Session Configuration Manager, users create their own customized local configurations settings for options, such as interface color, toolbars, menus, keyboard map or logon script.

In some previous versions of Web-to-Host, when the administrator made changes to Pro HTML session files, all user changes were reset (deleted).

Web-to-Host 6.7 provides a mechanism that preserves user changes. The SCM Wizard changes do not automatically delete the user's `.cph` file. Settings which only the user can set are not deleted when you, the administrator, change the HTML session files. This means users do not lose their customized environment with its colors, toolbars, and keyboard mappings.

This chapter lists the conditions that determine which configuration file takes precedence, if both an HTML session files and a user `.cph` file exist. It also explains how the configuration file is handled when included within a distribution package.

Rules defining Pro behavior

This section lists the rules for determining the settings implemented - default settings in HTML session files or user customized `.cph` settings.

No user configuration (.cph) file exists

> The first time the user opens a session no user `.cph` file exists. Consequently, the user receives the options defined in the Session Configuration Manager.

Existing user configuration (.cph) file

> When a user `.cph` file exists, the following rules apply:
>
> - If a `.cph` file exists, but no particular option is enabled, the user receives the default options set in the Session Configuration Manager. This is because you have not given the user permission to modify options. For example, if a user `.cph` file exists but you did not select **Enable Edit Options**, the user cannot create a customized configuration with features, such as word wrap or type ahead. The user is required to use the values set in the HTML session file.
> - If a `.cph` file exists and a particular option is enabled, the user can customize the configuration. For example, if **Enable Edit Options** is selected, the user can create a personalized environment that allows features, such as word wrap, type ahead, and keyboard auto reset. In this case, if you make changes to the HTML session file including those features which the user has customized, the user `.cph` file is not deleted and the customized environment remains in effect.
>
>   To enforce the use of the default HTML settings, you should disable the relevant option, for example, **Enable Edit Options**. Then the HTML settings override user settings for those options only. All other user configurations remain in effect.

User configuration files in a distribution package

As an administrator you can create a user `.cph` file from the session's HTML configuration and include it in a distribution package. This means the user starts with a customized, pre-configured session. It also means that you can provide the user with more configurable client options than you can assign using the Session Configuration Manager.

You can enable a particular client option, modify its settings using the option dialog, insert the session configuration file into a distribution package, then optionally disable the option (depending on whether you want to allow further user editing).

For example, selecting **Enable Edit Options** in the Session Configuration Manager allows you to open the **Edit Options** dialog box within a session and choose clipboard and parsing options that are not part of the Session Configuration Manager. The additional settings are added to the user `.cph` file. Then you can associate the session `.cph` file to a distribution package. If you want to maintain standardization, you can disable edit options.

In all cases, if you modify the distribution package, the new user configuration replaces the user's previous file, deleting all user settings.

User Data File Locations

OnWeb Web-to-Host stores user data on the client in a location specified by the user's environment. This location is determined by several environmental variables, such as the client operating system and browser, and whether roaming user profiles are enabled.

Roaming profile support for Pro and Java sessions

While normal Windows profiles store user environment settings on the client workstation, roaming user profiles store this information on their server. When a user logs on to the server, the roaming profile is downloaded to the client workstation. When the user logs off the server, the roaming profile (along with any changes) is uploaded back to the server. This scenario enables the user to work on different client workstations while using the same environment settings.

Web-to-Host supports roaming user profiles for Pro and Java client sessions. Users with roaming profiles can access their custom settings (such as keyboard maps and macros) when running Pro and Java sessions on various workstations.

Default paths for user data files

This section lists the user data file locations for a client workstation with a default Windows installation.

Pro sessions using Internet Explorer

If Rumba PC-to-Host has been previously installed on the client workstation, Web-to-Host stores user data files in the same location. If not, these locations are read from the Windows registry.

- **Windows 2003 and Windows XP:**

  Roaming path:

  `c:\Documents and Settings\<user_name>\Application Data\Micro Focus\Rumba`

  Local path:

  `c:\Documents and Settings\<user_name>\Local Settings\Application Data\Micro Focus\Rumba`

- **Windows Vista, Windows 7 and 8:**

  Roaming path:

  `c:\Users\<user_name>\AppData\Roaming\Micro Focus\Rumba`

  Local path:

  `c:\Users\<user_name>\AppData\Local\Micro Focus\Rumba`

You can use the MSI Packager to modify default user data file locations. For more information on the MSI Packager see the online help supplied with the utility.

Java sessions using Internet Explorer, Firefox, and Chrome

The Internet Explorer locations are the same as for the Pro sessions using Internet Explorer.

For Java sessions using Firefox or Chrome:

- **Windows Server 2003 and Windows XP:**

  Windows Server 2003 and Windows XP use the USERPROFILE environment variable.

  Roaming path:

  ```
  c:\Documents and Settings\<user_name>\Application Data\Micro Focus\Rumba
  ```

  Local path:

  ```
  c:\Documents and Settings\<user_name>\Local Settings\Application Data\Micro
  Focus\Rumba
  ```

- **Windows Vista, Windows 7 and 8:**

  Roaming path:

  ```
  c:\Users\<user_name>\AppData\Roaming\Micro Focus\Rumba
  ```

  Local path:

  ```
  c:\Users\<user_name>\AppData\Local\Micro Focus\Rumba
  ```

Creating a Trace

The Trace utility is a diagnostic tool for troubleshooting host communications and connectivity problems. With this utility you can trace activity within host software or other standardized components linked to OnWeb Web-to-Host. This chapter describes how to use the Trace utility to get a binary trace that can be sent to Micro Focus Technical Support for additional help troubleshooting your problems.

The Trace utility is supplied with the Java emulators. However, it must be installed separately for Pro.

Setting trace in Java Sessions

Java tracing is enabled through a set of parameters configured in the Session Configuration Manager. In all Java display and printer sessions, tracing is controlled from the **Custom Options** page. Tracing in these emulations is at two levels.

- Host Interface Tracing - captures Telnet data that flows between the emulator and the host.
- Session Tracing - captures the emulator specific data stream data.

The following parameters must be entered with a value of either `True` or `False` in the **Value** column:

- `EnableHostInterfaceTracing` and `EnableSessionTracing` determine if these levels are captured.
- `HostInterfaceTraceFile` and `SessionTraceFile` specify the path where the trace files are written and the name assigned to them. If they are left blank, trace data is written to the Java console (when enabled).
- `EnableTraceControlButtons`, when set to `True`, adds **Record**, **Stop**, and **Pause** buttons to the emulator's toolbar.
- `LogMaskHidden`, when set to `True`, replaces sensitive data in hidden fields with spaces.

When tracing is enabled, but `EnableTraceControlButtons` is not set to `True`, tracing is always on, and begins as soon as the emulator initiates its connection.

> **Notes:**
> - The Java UNIX display does not have a **Customs Options** page. Use the **Trace Options** page to set all trace parameters.
> - For Java AS/400 File Transfer, tracing is set from the **General Options** page. Clicking **Enable Trace** results in a new trace control button on the emulator's toolbar.

Setting trace in Pro Sessions

Pro uses the Rumba Trace utility that comes with Rumba as standard. If Rumba is installed, use its trace utility.

If Rumba is not installed, you can download the Trace utility from the server hosting OnWeb Web-to-Host. Type the following URL into the address bar of any Web browser.

```
http://<servername>/w2hlegacy/utils/installrumbatrace.exe
```

Important: Before starting the procedure, close all applications. If you are using Rumba, make sure it is closed. Be sure there are no blue and red icons in the tray bar.

To take a correct binary trace:

1. Select **Start** > **Programs** > **Micro Focus Rumba** > **Rumba Tools** > **Micro Focus Rumba 9.3 Trace**.
2. On the menu bar, select **Options** > **Configuration**.
3. On the **API Selection** page, click **Select All**. After all entries have been selected, click **Reset All**.
4. On the **Output** page, in the **Formatted Output** section, select **Display**.
5. In the **Binary Output** section select **Binary File**. The box next to the option becomes available.
6. Enter the full path for the binary file being created (or browse to it). For example, you might assign the file the call log number, `c368758.bin`. All file names should end with the extension `.bin`.
7. Click **OK.**
8. Minimize the **Rumba Trace** window that appears.
9. Run the Rumba application that is causing the problem as you normally would, starting from the connection (for example, Rumba Display, or Printer). Let the program run until the problem appears (error message, session hanging or any other problem).
10. Log off and disconnect from the host.
11. Maximize the **Rumba Trace** window.
12. Select **File** > **Exit**.
13. Send the binary file you created in Step *6* on page 39 by email to Micro Focus Technical Support.

Contacting Micro Focus

Micro Focus is committed to providing world-class technical support and consulting services. Micro Focus provides worldwide support, delivering timely, reliable service to ensure every customer's business success.

All customers who are under a maintenance and support contract, as well as prospective customers who are evaluating products are eligible for customer support. Our highly trained staff respond to your requests as quickly and professionally as possible.

Visit *http://supportline.microfocus.com/assistedservices.asp* to communicate directly with Micro Focus SupportLine to resolve your issues or e-mail *supportline@microfocus.com*.

Visit Micro Focus SupportLine at *http://supportline.microfocus.com* for up-to-date support news and access to other support information. First time users may be required to register.

Information needed by Micro Focus SupportLine

When contacting Micro Focus SupportLine, please include the following information, if possible. The more information you can give, the better Micro Focus SupportLine can help you.

- The name and version number of all products that you think might be causing an issue.
- Your computer make and model.
- System information such as operating system name and version, processors, and memory details.
- Any detailed description of the issue, including steps to reproduce the issue.
- Exact wording of any error messages involved.
- Your serial number. To find this number, look in the subject line and body of your Electronic Product Delivery Notice e-mail that you received from Micro Focus.

Additional information needed by Micro Focus SupportLine

If reporting a protection violation, you might be asked to provide a dump (`.dmp`) file. To produce a dump file, use the **Unexpected Error** dialog box that is displayed when a protection violation occurs.

Unless requested by Micro Focus SupportLine, leave the dump setting as `Normal` (recommended), click **Dump**, then specify a location and name for the dump file. Once the dump file has been written, you can e-mail it to Micro Focus SupportLine.

You may also be asked to provide a log file created by the Consolidated Tracing Facility (CTF) - a tracing infrastructure that enables you to quickly and easily produce diagnostic information detailing the operation of a number of Micro Focus software components.

Tell Us What You Think

We welcome your feedback regarding Micro Focus documentation.

Send feedback about this Help documentation.

Click the above link to e-mail your comments to Micro Focus.