IBM WebSphere Host On-Demand Version 7.0

Planning, Installing, and Configuring Host On-Demand

SC31-6301-00

IBM WebSphere Host On-Demand Version 7.0

Planning, Installing, and Configuring Host On-Demand

SC31-6301-00

Note

Before using this information and the product it supports, read the information in Appendix D, “Notices” on page 151.

Fourth Edition (September 2002)

This edition applies to Version 7.0 of IBM® WebSphere Host On-Demand (program number 5648–E81) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this book

The *Planning, Installing, and Configuring Host On-Demand* guide (which replaces the Host On-Demand *Getting Started* guide) helps you to plan for, install, and configure the Host On-Demand program. This book is written for administrators. It contains three major parts.

Part 1, “Planning for Host On-Demand” on page 1 gives you information about Host On-Demand for you to consider before installation and deployment. For example, which server platform will you use? Do you want to take advantage of any Java 2 functions? Which deployment model will you use? How will you handle security?

Part 2, “Installing, upgrading, and uninstalling Host On-Demand” on page 45 offers step-by-step procedures based on each operating system.

Part 3, “Configuring Host On-Demand” on page 71 describes different configuration models to specify how session configuration information is defined and managed, how to dynamically modify session configuration information, how to customize new clients, and how to deploy Host On-Demand to your users.

After you install and configure Host On-Demand, use the Online Help to learn how to define sessions and perform other administrative tasks.

The *Planning, Installing, and Configuring Host On-Demand* is also available in PDF on the CD-ROM and the Host On-Demand library page at www.ibm.com/software/webservers/hostondemand/library.html.

About the other Host On-Demand documentation

In addition to the *Planning, Installing, and Configuring Host On-Demand* guide, Host On-Demand also provides other sources of information to help you use the product. To access the documentation described here, go to the Host On-Demand library page at www.ibm.com/software/webservers/hostondemand/library.html. Most of the documentation is also included on the Host On-Demand product or Toolkit CD-ROMs.

- *Online Help*. The Online Help is the primary source of information for administrators and users after Host On-Demand installation is complete. It provides detailed steps on how to perform Host On-Demand tasks. A table of contents and an index help you locate task-oriented help panels and conceptual help panels. While you use the Host On-Demand graphical user interface (GUI), help buttons bring up panel-level help panels for the GUI.
- *Program Directory*. The program directory instructs you on how to install Host On-Demand on the z/OS and OS/390 platforms.
- *Readme file*. This file, readme.html, contains product information that was discovered too late to include in the product documentation.
- *Host Printing Reference*. After you configure host sessions, use the Host Printing Reference to enable your users to print their host session information to a local or LAN-attached printer or file.
- *Session Manager API Reference*. This book provides JavaScript APIs for managing host sessions and text-based interactions with host sessions.

- *Toolkit Getting Started*. This book explains how to install and configure the Host On-Demand Toolkit, which is shipped with the Host Access Client Package, but is installed from a different CD-ROM than the Host On-Demand base product. The Host On-Demand Toolkit complements the Host On-Demand base product by offering Java beans and other components to help you maximize the use of Host On-Demand in your environment.
- *Host Access Beans for Java Reference*. This book is part of the Host On-Demand Toolkit. It serves as a reference for programmers who want to customize the Host On-Demand environment using Java beans and create macros to automate steps in emulator sessions.
- *Host Access Class Library Reference*. This book is part of the Host On-Demand Toolkit. It serves as a reference for programmers who want to write Java applets and applications that can access host information at the data stream level.
- *J2EE Connector Reference*. This book is part of the Host On-Demand Toolkit. It serves as a reference for programmers who want to write applets and servlets that access Java 2 Enterprise Edition (J2EE) compatible applications.
- *Host On-Demand Redbooks*. The Host On-Demand Redbooks complement the Host On-Demand product documentation by offering a practical, hands-on approach to using Host On-Demand. Redbooks are offered ″as is″ and do not always contain the very latest product information. For the most up-to-date list of all Host On-Demand Redbooks, visit the Host On-Demand library page at http://www.ibm.com/software/webservers/hostondemand/library.html.

Conventions used in this book

The following typographic conventions are used in *Planning, Installing and Configuring Host On-Demand*:

Table 1. Conventions used in this book

Convention	**Meaning**
`Monospace`	Indicates text you must enter at a command prompt and values you must use literally, such as commands, functions, and resource definition attributes and their values. Monospace also indicates screen text and code examples.
Italics	Indicates variable values you must provide (for example, you supply the name of a file for *file_name*). Italics also indicates emphasis and the titles of books.
Return	Refers to the key labeled with the word Return, the word Enter, or the left arrow.
>	When used to describe a menu, shows a series of menu selections. For example, “Click File > New” means “From the File menu, click the New command.”
	When used to describe a tree view, shows a series of folder or object expansions. For example, “Expand HODConfig Servlet > Sysplexes > Plex1 > J2EE Servers > BBOARS2” means: 1. Expand the HODConfig Servlet folder 2. Expand the Sysplexes folder 3. Expand the Plex1 folder 4. Expand the J2EE Servers folder 5. Expand the BBOARS2 folder
Java 1	In this book, Java 1 means implemented in a Java 1.1.x JVM.
Java 2	In this book, Java 2 means implemented in a 1.3 and later JVM.

✎ This graphic is used to highlight notes to the reader.

💡 This graphic is used to highlight tips for the reader.

Part 1. Planning for Host On-Demand

Chapter 1. Introducing WebSphere Host On-Demand

What is WebSphere Host On-Demand?

IBM WebSphere Host On-Demand provides cost effective and secure browser-based host access to users in intranet-based and extranet-based environments. Host On-Demand is installed on a Web server, simplifying administrative management and deployment, and the Host On-Demand applet is downloaded to the client browser providing user connectivity to critical host applications and data.

Host On-Demand supports emulation for common terminal types, communications protocols, communications gateways, and printers, including the following:

- TN3270 and TN3270E terminals
- TN5250 terminals
- VT52, VT100, VT220, VT320, and VT420 terminals
- File Transfer Protocol (FTP)
- Customer Information and Control System (CICS) Transaction Gateway
- TN3270E and TN5250 printers

You can use the Java component-based Host Access Toolkit to create customized e-business applications. This Toolkit contains a rich set of Java libraries and application programming interfaces: Host Access Class Library (HACL), Host Access Beans for Java, and Java 2 Enterprise Edition (J2EE) connectors. Host On-Demand also includes Database On-Demand, which provides an interface for sending Structured Query Language (SQL) queries to IBM DB2 databases hosted on iSeries systems.

How does Host On-Demand work?

The following figure shows how a Host On-Demand system works. Host On-Demand is a client/server system. Host On-Demand clients are Java applets that are downloaded from the Web server to a Web browser on a remote computer.

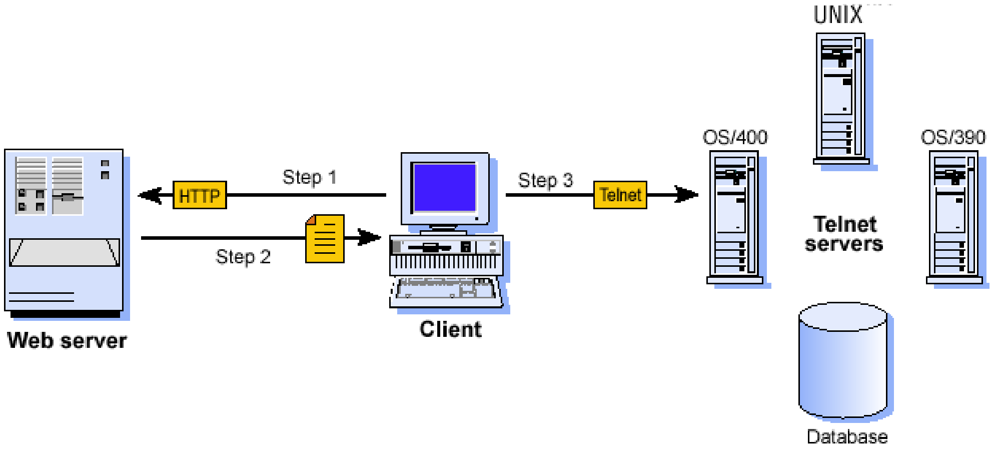

Figure 1. How Host On-Demand works

Step 1. The user opens a browser and clicks a hyperlink.

Step 2. IBM WebSphere Host On-Demand applet downloads to the client workstation.

Step 3. When the applet is downloaded, IBM WebSphere Host On-Demand connects directly to any Telnet server to access host applications.

Session information is configured in the HTML file or Host On-Demand configuration server. For more information about the configuration server, see Chapter 3, "Planning for deployment" on page 19.

Host On-Demand client applets can be run as download clients or cached clients. Download clients are downloaded from the Web server every time they are used. Cached clients are downloaded from the Web server and stored on the client computer. After the initial download, the cached client is loaded from the local machine. The cached client checks the Host On-Demand server for new versions of the client and automatically downloads the updated version.

Host On-Demand includes the following administrative components:

- The Deployment Wizard, a tool for creating emulator client HTML files. The Deployment Wizard enables administrators to quickly and easily build Host On-Demand HTML files that are customized for an organization's needs.
- Administration clients that can be used by system administrators to define common sessions, create users and groups, and perform other administrative tasks on the Host On-Demand server.

In addition, a number of predefined clients are also supplied with Host On-Demand to demonstrate Host On-Demand's client functions for users and administrators (for example, emulation, Database On-Demand, cached client removal, and problem determination utilities).

Why use Host On-Demand?

A cost-effective approach to connectivity

You can reduce maintenance costs and increase your return on investment by installing Host On-Demand on a Web server, eliminating the need to manage individual user desktops.

Since the applets reside on a server and are downloaded to Web browsers when needed, you no longer have to schedule maintenance and upgrades. Upgrade the software on the server and users can receive the upgrade the next time they access the client applet.

Centralized management of configuration data

Administrators can centrally define and control all session configuration information available to their users, including connection options, security features, macro definitions, keyboard specifications, and color mappings. Furthermore, administrators have full control over which fields the user can or cannot modify, and can choose where user updates should be stored.

Connect directly to any Telnet server

With Host On-Demand, the client applet contains the emulation functionality. This eliminates the need for a middle-tier server —a performance and security issue. Once the applet is served to the client, it is easy to connect directly to any standard Telnet server that provides the best access to the required data. You can change the Telnet connection as often as user requirements for new data change. You can access many host sessions concurrently. Host On-Demand minimizes capacity restrictions by eliminating the need for a middle-tier server. To see how this works, refer to Figure 1 on page 3.

Browser-based user interface

The browser-based access of Host On-Demand gives you a simple way to reach critical host applications and data, without requiring you to install any software on your workstation. Host On-Demand uses the power of Java technology to open the doors to your host system whenever you need it, wherever you need it, directly from your browser. Just click on a hyperlink to launch the Host On-Demand Java applet. This Web-to-host connectivity solution provides secure Web-browser access to host applications and system data through Java-based emulation, so you can take existing host applications to the Web without programming. Because Host On-Demand is Java-based, its interface has the same look-and-feel across various types of operating environments. Host On-Demand also provides a default graphical user interface (GUI) to simplify the experience for users who are unfamiliar with traditional ″green screens.″

Supports many different platforms and network environments

Host On-Demand servers and clients are supported on a wide variety of platforms and can be used over any TCP/IP network. This gives you a great deal of flexibility in setting up your system and enables Host On-Demand to be deployed in your computing environment without having to purchase expensive new hardware.

Java 1 and Java 2 support

Host On-Demand is compatible with browsers that support either the Java 1 or Java 2 standards. In addition, some new features of Host On-Demand take advantage of capabilities offered by Java 2.

Supports many national languages

Host On-Demand is available in 23 languages, including double-byte character set (DBCS) languages. Support for the European currency symbol, as well as keyboard and code page support for many more languages such as Arabic, Hebrew and Thai, is also provided. All language versions are available on the same media, and multiple language versions can be accessed concurrently.

Secure connections

Using Transport Layer Security (TLS) version 1.0 and Secure Sockets Layer (SSL) Version 3.0, Host On-Demand extends secure host data access across intranets, extranets, and the Internet. Mobile workers access a secure Web site, receive authentication and establish communication with a secure enterprise host. With client and server certificate support, Host On-Demand can present a digital certificate (X.509, Version 3) to the Telnet server - such as IBM Communications Server for Windows NT Version 6 or later, or IBM Communications Server for OS/390 Version 2.6 or later - for authentication.

Host On-Demand can also be configured for use in environments that include firewalls. Firewall ports need to be opened for the functions defined in your Host On-Demand session definitions. See “Using Host On-Demand with a firewall” for more details.

Create custom HTML files

Host On-Demand includes a Deployment Wizard that enables you to create custom HTML files. These files can tailor the content of the client and the function necessary to meet the needs of specific groups of users. For more information about the Deployment Wizard, see Chapter 10, “Configuring Host On-Demand emulator clients” on page 73.

Toolkit for creating new e-business applications

Host On-Demand includes the Java component-based Host Access Toolkit for creating customized e-business applications. This Toolkit contains a rich set of Java libraries and application programming interfaces, including the Host Access Class Library (HACL), Host Access Beans for Java, and Java 2 Enterprise Edition (J2EE) connectors.

HACL provides a non-visual API for interacting with back-end host machines running applications originally designed for human interaction. Host applications rely on readable character presentation, formatted fields, color-coding and keyboard responses. HACL provides specialized classes for functionalities needed to mimic traditional interaction with a series of host screen presentations (green screens). HACL contains no GUI (visible component) classes.

Host Access Beans for Java provide an easy way to develop applications for visual and non-visual environments. Developers can present to the user different pieces of an emulator to quickly provide core functions. For example, the Terminal and Screen beans display the actual screens and OIA (Operator Information Area) information generated by the host. Because Host Access Beans for Java are components themselves, rapid development of applications based upon this library is possible. If the API of the beans is not sufficient for an application’s needs, the underlying HACL API is accessible.

The Host On-Demand J2EE Connector provides access to 3270, 5250, Customer Information and Control System (CICS), and Virtual Terminal (VT) hosts from the Internet. The Host On-Demand J2EE Connector is a Java programming interface that conforms to the J2EE Connector Specification Version 1.0. This translates to a standard set of services for accessing any system that is J2EE Connector architecture compliant, whether it be the mainframe-based host systems or any other system.

Host On-Demand J2EE Connector provides a set of Resource adapters that communicate to 3270, 5250, CICS, and VT hosts. These resource adapters are deployed to a conforming application server, such as IBM WebSphere Application Sever. The users can write Web applications using the APIs provided in Host On-Demand J2EE Connector via WebSphere Studio Application Developer Integration Edition.

Support for WebSphere Portal

Host On-Demand can run as a portlet on Portal Server, a component of WebSphere Portal. Portal Server has sophisticated desktop management and security features that offer administrators more control over user access rights and end users control over the appearance and arrangement of the portal desktop.

Administrators can create customized Host On-Demand portlets quickly and easily using the Deployment Wizard and then load them directly into Portal Server. (Note that Portal Server is a separate product and requires independent installation.)

Connections to DB2 databases on iSeries

Database On-Demand is included with Host On-Demand to provide access to DB2 information stored on iSeries computers using a Java Database Connectivity (JDBC) driver. Database On-Demand is a Java applet that allows you to perform Structured Query Language (SQL) requests to iSeries databases through a JDBC driver.

What's new?

Getting the latest information on Host On-Demand

For the most recent information on Host On-Demand 7, see the `readme.html` file.

For up-to-date product information, go to the Host On-Demand Web site at `http://www.ibm.com/software/webservers/hostondemand`.

For the latest technical hints and tips for Host On-Demand, go to the `Host On-Demand Hints and Tips site`.

To subscribe to the Software Support Bulletin, go to `http://www.ibm.com/software/network/support`.

New features in Host On-Demand 7

The following functions and enhancements were added to Host On-Demand 7:

User productivity enhancements

Customizable toolbar: Administrators and users can customize the toolbar buttons used for Host On-Demand sessions. You can rearrange the buttons on the toolbar, as well as add or edit toolbar buttons to assign a keyboard function to a particular toolbar button. You can also choose your own icons for custom buttons. After customizing the toolbar, settings are saved for future sessions. Refer to `Customize Toolbar` in the online help for more information.

Macro enhancements: With the macro enhancements in Host On-Demand 7, you can:

- Create and update variables within a Host On-Demand macro and use the variables anywhere in the macro. You can also specify a screen position, by row and column, and store text from the field containing the specified position.
- Place conditions around actions to be performed when a macro screen is recognized.
- Assign an arithmetic expression to a variable as the initial value, for example, 1 + 2a. Arithmetic operations can be performed on numbers, integer variables, double variables, field variables, and string variables. For more information about the operations that Host On-Demand supports, see `Variables` in the online help.

- Start a macro from another macro and run programs from a Host On-Demand macro. Refer to `Editing a Macro` in the online help for more information.

Session inactivity timeout: When configuring sessions, administrators can set an inactivity timeout for 3270 or 5250 display/printer sessions or VT sessions. After the session connection has been idle for the specified number of minutes, the connection will be terminated. Refer to `Advanced Tab` in the online help for more information.

Accessibility features: Based on Section 508 of the US Rehabilitation Act, Host On-Demand offers new accessibility features to help users who have physical disabilities, such as restricted mobility, limited or no vision, or limited or no hearing, use host sessions successfully. Features include keyboard equivalents for all actions (mouseless operation), support for display system settings for size, font, and color for user interface controls, and descriptive text for selected graphics. Currently, not all features are available for all screens; for example, the Administration Clients and the InstallShield are not yet fully accessible. Accessibility features require Java 2. For more information, refer to "Accessibility issues" on page 24 in this guide or to `Accessibility` in the online help.

Associated printer session improvements: Improvements have been made to the 3270 client to reduce the risk of associated printer sessions being inadvertently shared by different users when logical units (LUs) are configured as pooled in the telnet server. The display session now more tightly controls whether an associated printer session is disconnected. Refer to `Advanced Tab` in the online help for more information.

Remap graphics colors (3270 only): This option allows host applications to remap graphics colors, in addition to text, on the screen. Refer to `Disable Functions: Preferences` in the online help for more information.

Arranging session icons: Clients can now arrange their configured sessions on the desktop by name or type. (This option is only available for the HTML-based and combined models in the Deployment Wizard.)

Administrators can also reorder session definitions when defining an HTML-based model file in the Deployment Wizard. The order in which sessions are defined determines the initial order in which users will see those sessions. Refer to `Starting Sessions with Bookmarks or Icons` in the online help for more information.

Custom Function Editor: Certain keyboard functions are predefined with Host On-Demand for remapping. The Custom Function Editor allows you to define and maintain new keyboard functions, called custom functions, without having to edit HTML and Java script files. These new functions may be mapped to key combinations, much like the predefined keyboard functions. Refer to `Custom Function Editor` in the online help for more information.

Display URL hot spots: Hot spots can now be displayed as underlined links or as three-dimensional buttons. Refer to `Help for displaying URLs` in the online help for more information.

Confirmation on exit: When a user attempts to close a current Host On-Demand session, a confirmation dialog will appear. If the user selects OK, the session will close. Refer to `Confirm on exit` in the online help for more information.

Print screen enhancements: Users with Java 2–enabled browsers can now specify page orientation and margins, add headers and footers, and suppress the print dialog box. Refer to `Print Setup Dialog Box` in the online help for more information.

Support for Start PC Command (STRPCCMD): Host On-Demand 5250 sessions support the Start PC Command (STRPCCMD). STRPCCMD allows you to launch an application on a personal computer that is attached to the host iSeries system. Refer to `Using the Start PC Command (STRPCCMD) in Host On-Demand` in the online help for more information.

Support for grid lines defined by DDS: DBCS 5250 display sessions now support grid functions that are defined by Data Description Specifications (DDS). Refer to `Enable ENPTUI` (Advanced tab) in the online help for more information.

Cached client improvements: Administrators can now specify a separate upgrade percentage for peak and off-peak demand periods for the Web server to enable clients to more easily upgrade. In addition, when clients install or upgrade the cached client, they are presented with a download size and an estimated download time so they can assess whether to proceed with or postpone the install or upgrade. Refer to `Cache Options` in the online help for more information.

Technology improvements

Java 2 support on the client: Clients running the Java 2 plug-in are now supported. Certain Host On-Demand 7 features require Java 2. For more information, see Chapter 4, “Planning for Java 2 on the client” on page 23.

Adobe Portable Document Format (PDF) printing: Users can now create Adobe PDF versions of host documents for printing from 3270 printer sessions. This feature allows users to select the option to display files using the Adobe Acrobat reader with the Adobe Acrobat plug-in installed. Refer to `Creating Adobe PDF Files` in the Host Printing Reference for more information.

Auto Input Method Editor option for generating DBCS characters: Host On-Demand now provides the option to select the Auto Input Method Editor (IME) feature on the Language tab when configuring 3270 and 5250 display sessions. IME is a front-end processor for generating DBCS strings. This function requires Java 2 and is available only in DBCS-enabled environments.

Host On-Demand also provides an On-the-Spot Conversion function, which displays ″In-Composition″ DBCS strings at the cursor position where users are inputting text in the application. This function requires Java 2 and is available only in DBCS-enabled environments. Refer to `Language Tab` in the online help for more information.

Session Manager APIs: The Host On-Demand Session Manager provides JavaScript APIs for managing host sessions and text-based interactions with host sessions. These APIs are intended to provide support for embedding host sessions in a Web page using JavaScript. See the `Host On-Demand Session Manager API Reference` for more information.

Socks 5 and HTTP proxy server support: Host On-Demand clients can use a proxy server to transparently access host systems that are behind a firewall. Both Socks proxy servers (Version 4 and Version 5) and HTTP proxy servers are supported.

Proxy server settings can be specified on a session-by-session basis or through the Web browser. A new tab, **Proxy server**, has been added to the session properties window to let you set proxy server properties for a session. Refer to `Proxy Server Tab` in the online help for more information.

Support for TLS version 1.0 security protocol: Host On-Demand supports version 1.0 of the Transport Layer Security (TLS) protocol. TLS is an open standards security protocol that is similar in function to SSL. The Security panel of the Session Properties page has been modified to allow either the TLS or SSL security protocols to be selected. TLS is the default session security protocol. For detailed information on TLS, see the description of the *TLS Protocol Version 1.0* at http://www.ietf.org/rfc/rfc2246.txt. For more information, refer to `Security Tab` in the online help.

Support for IBM WebSphere Portal

Host On-Demand can now be run as a portlet within the Portal Server component of WebSphere Portal. Administrators can use the Deployment Wizard to create custom Host On-Demand portlets with only the features they desire. Preconfigured sample portlets are available for download either from the Host On-Demand Service Key site at `http://www6.software.ibm.com/aim/home.html` on the Host On-Demand CSD Web page under Tools and Utilities or from the Portal Server portlet catalog at `http://www7b.software.ibm.com/webapp/portlets/portletemarketplace`.

For more information about Host On-Demand and WebSphere Portal, refer to Chapter 17, "Deploying Host On-Demand With WebSphere Portal" on page 123 in this guide.

Administrator improvements

Stand-alone Deployment Wizard installation: The Deployment Wizard can now be installed on Windows platforms using one of the following two approaches:

- The Host On-Demand CD for Windows has a Deployment Wizard installation option. Note that if you install Host On-Demand for Windows, you do not need to install the Deployment Wizard separately, because it will be installed automatically as part of the product.
- The Deployment Wizard installation image is also available on all Host On-Demand server platforms. You can download it from the server and install it on a Windows machine by accessing the HODMain_*xx*.html file, where *xx* is your two-letter language suffix. From here, select the link Deployment Wizard Installation Image for Windows.

For more information about installing the Deployment Wizard, refer to "Installing the Deployment Wizard" on page 61 in this guide.

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

Usability improvements for defining smaller clients: Administrators can now more easily define a smaller client. When components are selected for initial download on the Preload Options panel in the Deployment Wizard, the size requirements for each component, a running total of the size for all components selected, and the archive file relationships between components is displayed. Additionally, if the HTML-based model is being used, components can be automatically selected according to the sessions that are defined. Any component a user might be able to access will be included. For more information about how to define smaller clients, refer to `Preload Options` the online help.

Publishing Deployment Wizard files: You can now publish files generated from the Deployment Wizard to a location other than your Host On-Demand publish directory by specifying the URL of your Host On-Demand publish directory in the Codebase field on the Advanced Options panel. This name must either be a fully qualified URL, including the hostname (for example, http://your_HOD_server/hod_publish_dir_alias/), or a relative path (for example, /hod_publish_dir_alias/). This function makes future upgrades easier. For more information about how to publish files to another location other than your Host On-Demand publish directory, refer to "Backing up files and directories" on page 63 in this guide.

Customizing Web page appearance: Administrators can now customize the appearance of Host On-Demand Web pages created with the Deployment Wizard by using custom HTML templates. The custom HTML template is chosen in the Deployment Wizard at the time the Web page is created or edited. It can include a different banner, background, new images and text, forms, and JavaScript. For more information, refer to `Using Custom HTML Templates` in the online help.

Changing session runtime properties: A new administration client now allows administrators to easily change session runtime properties for the user, such as keyboard remapping, color definitions, and recording macros, by starting the sessions. For more information, refer to `Modifying a Session's Runtime Properties` in the online help.

Pasting sessions directly to users and groups: The administrator can now copy and paste new sessions to the Users/Groups window in the administration client. Refer to `Pasting to the Users/Groups Window` in the online help for more information.

Modifying session properties dynamically: Host On-Demand sessions are defined by the administrator and retrieved by the Host On-Demand client when a user accesses a Host On-Demand HTML file. The session properties that a user will see are fixed values and consist of a combination of the administrator's initial configuration and any user updates. However, there may be times when it would be useful with some HTML files, or with certain session properties, to dynamically set a value at the time that the HTML is accessed. This type of control allows you to set particular session property values based on information such as the IP address of the client or the time of day. For more information, refer to Chapter 14, "Modifying session properties dynamically" on page 95 in this guide.

FTP enhancements

FTP support for directory transfer: The Host On-Demand FTP client now supports transferring directories to and from the host. For more information about transferring files and directories, refer to `FTP client overview` in the online help.

FTP Transfer List Manager: A new Transfer List Manager toolbar in the FTP client allows you to create file or directory transfer lists. For more information, refer to `Transfer List Manager` in the online help.

FTP support for renaming files or directories before transfer: The Host On-Demand FTP client now supports renaming files or directories before they are transferred to the receiving file system. For more information about transferring files and directories, refer to `FTP client session window` in the online help.

FTP support for viewing server directory information: The Host On-Demand FTP client now allows you to view unparsed server directory information, including all attributes provided by the FTP server. For an overview of FTP, refer to `FTP client session window` in the online help.

FTP client support for OpenVMS: The Host On-Demand FTP client now supports the directory listing of OpenVMS and VMS operating systems, allowing you to connect to a VMS FTP server and browse through its files. For more information, see the FTP session properties `More Advanced Tab` in the online help.

Enhanced FTP client support for OS/390 or z/OS servers: The FTP client now supports listing the contents of MVS Services and HFS Services without changing the host type or defining two separate FTP sessions. For more information, see the FTP session properties `More Advanced Tab` in the online help.

FTP support for UTF-8 transfer type: The Host On-Demand FTP client now converts path names to UTF-8 when sending files or directories to the server and converts path names back to the local client encoding when receiving files or directories from the server. For more information, see the FTP session properties `More Advanced Tab` in the online help.

Language selection for FTP greetings and error messages: If you enable UTF-8 transfer type, you can select the language for FTP greetings and error messages from a list of languages supported by Host On-Demand. For more information, see the FTP session properties `More Advanced Tab` in the online help.

Chapter 2. Requirements

For updates to this information, refer to the Readme.

Server requirements

zSeries platform

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

iSeries platform

Table 2. iSeries server requirements

Server operating system	OS/400 (R) V4R5, V5R1, and V5R2. Recent cumulative service is recommended. Refer to the OS/400 Fixes, Downloads and Updates Web page for service information.
Disk space	410 MB DASD
Memory	256 MB memory or more. Refer to the iSeries Performance Capabilities Reference Web page for additional information about the impact of additional memory and Java performance
Supported Web servers	• Apache-based HTTP Server for iSeries • IBM HTTP Server for iSeries • Lotus Domino for iSeries
Java	IBM Java Toolbox Java Developer's Kit *BASE option and one of the following: • Option 4 - 1.1.8 • Option 5 - 1.3
All other requirements	TCP/IP Connectivity Utilities for iSeries QShell Interpreter

Windows platforms

Table 3. Windows server requirements

Server operating systems	• Windows NT 4.0 with SP5 or later • Windows 2000 Professional, Server, and Advanced Server • Windows XP Professional (32-bit) (Note: This should not be used for a large scale production server.)
Disk space	340 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.

Table 3. Windows server requirements (continued)

Supported Web servers (automatically configured)	• IBM HTTP Server • IBM Internet Connection Server • Lotus Go, Domino, and Domino Go • Microsoft Internet Information Server 3 and 4 • Microsoft Peer Web Services • Microsoft Personal Web Server
Java	Installed with Host On-Demand

AIX platform

Table 4. AIX server requirements

Server operating system	AIX (R) Version 4.3.3 and 5L 5.1
Disk space (installp image)	310 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed (including the additional security files).
Supported Web servers	• Apache Web Server • IBM HTTP Server
Java	JVM 1.1.8 or 1.3

You can obtain the latest AIX JVM from one of the following Web sites:

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

Solaris platform

Table 5. Solaris server requirements

Server operating system	Sun Solaris 2.6, 7, and 8
Disk space	278 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Supported Web servers	• Apache Web Server • IBM HTTP Server
Java	JVM 1.1.8 or 1.3

You can obtain the latest Solaris JVM from one of the following Web sites:

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

HP-UX platform

Table 6. HP-UX server requirements

Server operating system	HP-UX 10.20, 11.00, and 11.i
Disk space	278 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.

Table 6. HP-UX server requirements (continued)

Supported Web servers	- Apache Web Server - IBM HTTP Server
Java	JVM 1.1.8 or 1.3

You can obtain the latest HP-UX JVM from one of the following Web sites:

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

Linux and other Unix platforms

Table 7. Linux server requirements

Server operating systems	- Red Hat Linux 6.2, 7.0, 7.1, 7.2, and 7.3 - SuSE Linux 6.4, 7.0, 7.1, 7.2, 7.3, and 8.0 - Caldera 2.3 and 3.1 - TurboLinux 6.0, 6.5, and 7.0 - Unixware 7
Disk space	278 MB for an English-only installation. Add 4 to 8 MB for each additional national language to be installed.
Supported Web servers	- Apache Web Server - IBM HTTP Server
Java	JVM 1.3 or 1.4

You can obtain the latest Linux JVM from the following Web site:

```
http://www.ibm.com/java
```

When using Redhat Linux Version 7.0, make sure that the glibc package is at least Version 2.2-12. In addition, make sure the IBM JDK is at least J2RE 1.3.0 IBM Build cx130-20010207.

OS/2 platform

Table 8. OS/2 server requirements

Server operating system	- OS/2 (R) Warp Server Version 4 - OS/2 Warp Server for e-Business 4.5
Disk space	410 MB. The hard disk must be configured for HPFS.
Supported Web servers	Lotus Domino Go Web server for OS/2
Java	OS/2 JVM 1.1.8 or JVM 1.3.

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

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

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

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

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

Novell Netware platform

Table 9. Novell Netware server requirements

Server operating system	Novell NetWare Version 4.2, 5.1, and 6
Disk space	410 MB
Supported Web servers	Novell Web Server
Java	Novell Java Development Kit 1.1.8

You can obtain the latest Novell JDK at `http://www.developer.novell.com`. The JDK must be configured for long-filename support.

For users to load the client HTML files from a Novell server, their browsers might need to be configured not to use a proxy server. In addition, if users have a browser with a Java 2 plug-in, the IBM plug-in must be 1.3.0 or later and the Sun plug-in must be version 1.3.1 or later. The client applets do not successfully load if the plug-in is an earlier version.

Supported LDAP servers

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

- IBM LDAP Directory Server V2.1, V3.1.1 V3.2.1, V3.2.2
- IBM LDAP Server running on OS/390 V2R9, V2R10
- IBM LDAP Server running on z/OS V1R1, V1R2, V1R3, V1R4
- Netscape Directory Server V3.1 and V4.0 (Windows NT and AIX)

For more information on IBM’s LDAP Directory solution and to download a complimentary evaluation kit, go to `http://www.software.ibm.com/network/directory/`

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

Web servers

The following Web servers are supported:

- Websphere Application Server 3.5, 4.0
- Lotus Domino R5, R6
- Netscape iPlanet (JRun) V4.1
- iPlanet Web Server Enterprise Edition V6.0
- iPlanet Application Server V6.0
- IBM HTTP Server V1.3.6.2, V1.3.6.4, V1.3.12.6, V1.3.19.2, V2.0

Miscellaneous software

- License Use Management Version 4.5
- IBM WebSphere Portal Family 2.1
- IBM WebSphere Portal for Multiplatforms 4.1
- Acrobat Reader (Acrobat) version 4.0 or newer (Note: Acrobat version 5.0 or newer is required for DBCS PDF support.)

Client requirements

For updates to client requirements, refer to the Readme file, readme.html.

Supported operating systems

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

- Windows 95
- Windows 98
- Windows Millennium Edition (ME)
- Windows NT 4.0 with SP5 or later
- Windows 2000 (Professional)
- Windows XP Professional and Home Edition (32-bit version)
- AIX 4.3.3, AIX 5L 5.1
- OS/2 Warp 4
- Sun Solaris 2.6, 7, and 8
- HP-UX 10.20, 11.00, and 11i
- Red Hat Linux 6.2, 7.0, 7.1, 7.2, and 7.3
- SuSE Linux 6.4, 7.0, 7.1, 7.3, and 8.0
- Caldera 2.3 and 3.1
- TurboLinux 6.0, 6.5, and 7.0
- Windows Terminal Server Version 4
- Windows Terminal Services for 2000
- Netstation V2R1M0
- Citrix Metaframe 1.8 for Windows Terminal Server 4.0 and 1.8 for Windows 2000 Server
- Citrix Metaframe XP (Versions s,a,e) for Windows

A local client is supported only on Windows NT, Windows 2000, Windows 95, Windows 98, and Windows Millenium.

Supported browsers

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

- Netscape Navigator 4.6, 4.7, 6.1, 6.2
- Netscape Navigator (OS/2) 4.61
- IBM Web Browser for OS/2 V1.2
- Microsoft Internet Explorer 4.01 with SP1, 5.0 or 5.1, 5.5, 6.0
- Sun and IBM Java plug-in 1.3, 1.3.1, and 1.4

If you are using a Java 2-enabled Web browser, such as Netscape 6.x or the IBM Web Browser for OS/2, several restrictions on Host On-Demand functions apply when using the predefined HTML pages (HOD.html). For more information on these limitations, see Chapter 4, “Planning for Java 2 on the client” on page 23.

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

Chapter 3. Planning for deployment

Host On-Demand provides access to host applications from a Web browser. The browser downloads the Host On-Demand Java applet from the Web server and then connects to any Telnet server to access host applications. The Host On-Demand applet needs configuration information to determine which host to connect to and other host session properties. This configuration information can be provided to the Host On-Demand applet from an HTML file or by using the Host On-Demand configuration server. The configuration server is a part of Host On-Demand that centrally stores session configuration information and user preferences by user and group IDs. Users then access session information and user preferences by contacting the configuration server. The configuration server is managed through the administration client. For information on configuring the Host On-Demand configuration server, see the online help.

You can create custom client HTML files using the Deployment Wizard. When creating these HTML files, you can choose from three different configuration models to specify how session configuration information and user preferences (for example, changes users make to session size and location, colors, etc.) are defined and managed: the HTML-based model, the configuration server-based model, and the combined model.

These models are described below. For detailed information on each model and benefits and limitations to using each model, see the online help.

Understanding the HTML-based model

If you choose the HTML-based model, all host session configuration information is contained in the HTML file itself, and nothing more is needed to define host sessions. Therefore, you are not required to use the configuration server to specify sessions, which means you do not have to open up a port on your firewall. If you allow users to save changes to the host session configuration information, their changes are stored on the local file system where the browser is running.

This option of defining configuration information in the HTML files is only available in clients that are created using the Deployment Wizard.

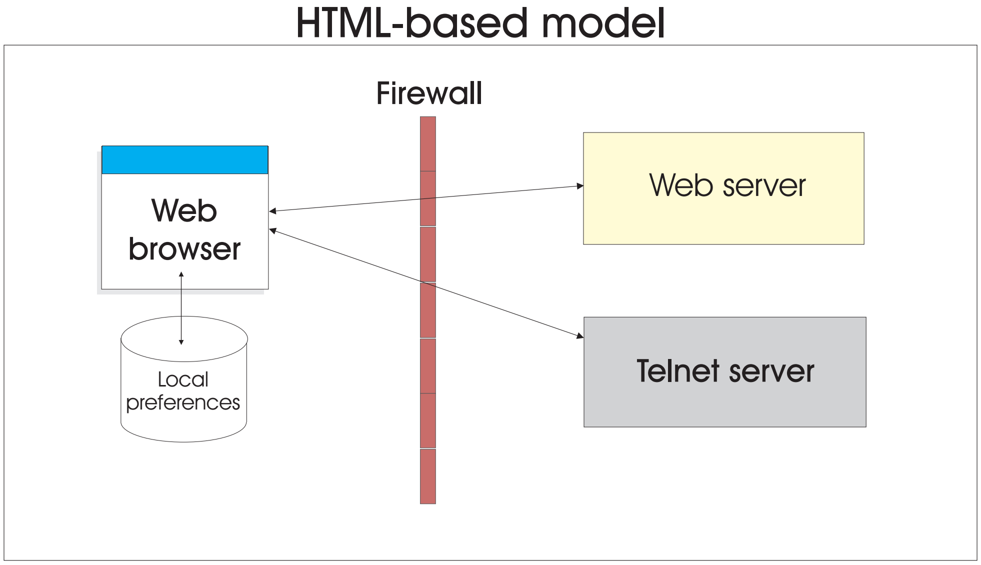

Figure 2. HTML-based model

Understanding the configuration server-based model

In the configuration server-based model, host session information is maintained on the configuration server using the Administration client, and the information is defined using a user and group structure. By default, the configuration server stores its data locally on the Host On-Demand server machine, though it can be configured to use LDAP instead. Users access their configurations using either custom HTML files created in the Deployment Wizard or by using one of several HTML files that are provided as part of Host On-Demand. User IDs are defined in the configuration server, and in most cases the user needs to log on to the Host On-Demand server before viewing his sessions. If administrators allow users to save changes, user preferences are stored in the configuration server by user ID. Because their customizations are saved on the configuration server, this model may be the best choice if users need to access their sessions from multiple machines.

By default, the Web browser communicates directly to the configuration server. If you are communicating through a firewall, you will need to open the configuration server's port on the firewall. You can also use the configuration servlet, through which the Web browser communicates with the configuration server. The connection from the Web browser to the configuration servlet is over HTTP or HTTPS, so the configuration server's port does not need to be opened on the firewall. See Configuring the configuration servlet for more information on using the configuration servlet.

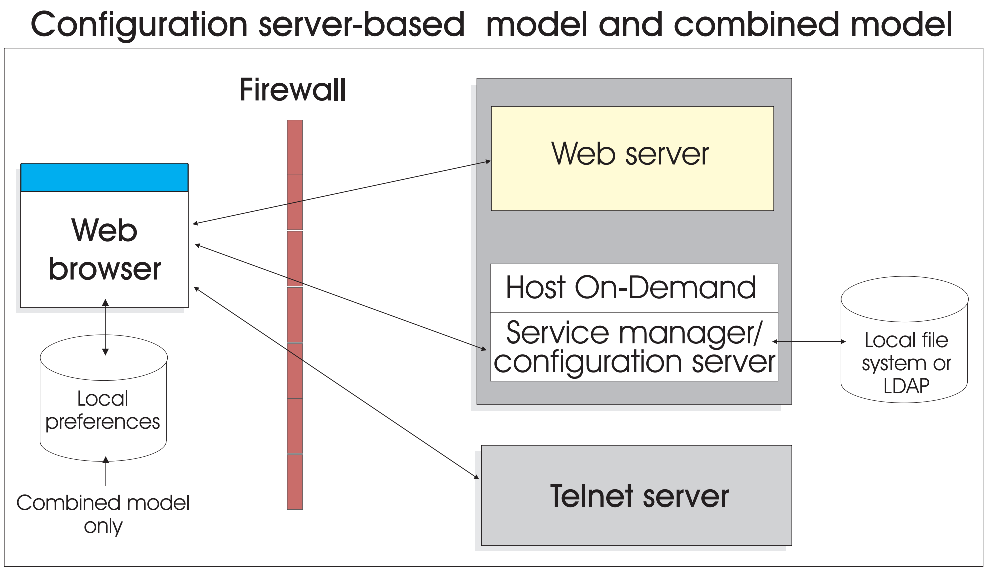
Configuration server-based model and combined model
Firewall
Web browser
Local preferences
Combined model only
Web server
Host On-Demand
Service manager/ configuration server
Local file system or LDAP
Telnet server

Figure 3. Configuration server-based model and combined model

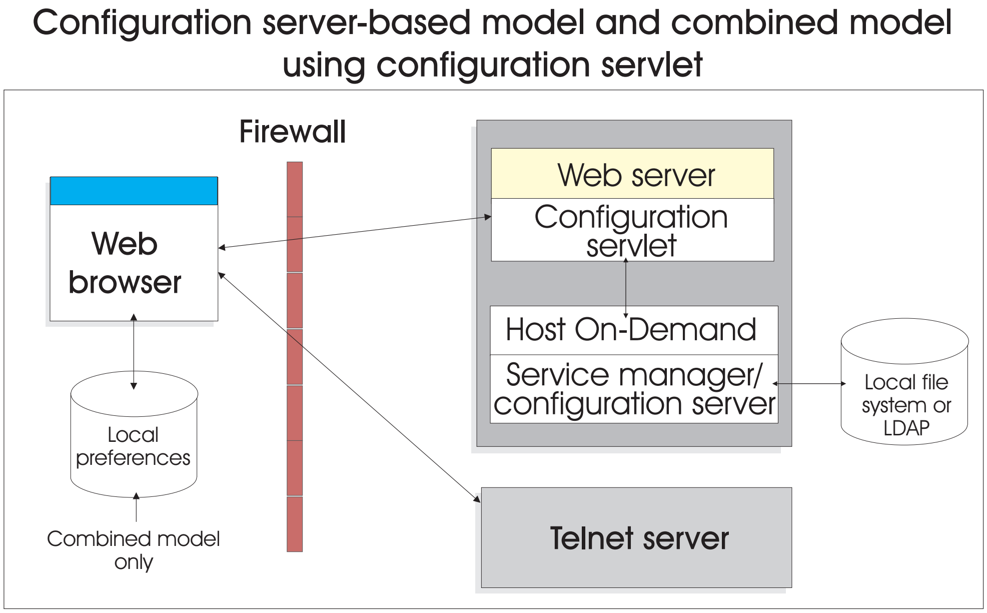
Configuration server-based model and combined model using configuration servlet
Firewall
Web browser
Local preferences
Combined model only
Web server
Configuration servlet
Host On-Demand
Service manager/ configuration server
Local file system or LDAP
Telnet server

Figure 4. Configuration server-based model and combined model using configuration servlet

Understanding the combined model

Host On-Demand supports a combined model, where the host session information is defined in the configuration server (like the configuration server-based model) and user updates are saved on the user's machine (like the HTML-based model). In addition, like the HTML-based model, users of the combined model do not need to log on to the Host On-Demand server to view their sessions.

Client deployment considerations

Additionally, for client deployment considerations, you need to decide whether to use cached or download clients (see Chapter 12, “Using Host On-Demand emulator clients” on page 81) and which version of Java to use (see Chapter 4, “Planning for Java 2 on the client” on page 23).

Chapter 4. Planning for Java 2 on the client

Java 2 upgrade planning issues

With more emphasis being placed on Java 2 technology, Host On-Demand is now taking advantage of features available with Java 2-enabled Web browsers.

Several functions are available with Host On-Demand 7 that require Java 2 on the client:

- Auto IME/On-the-Spot Conversion
- Accessibility
- Print Screen Enhancements

Existing Java 1 Host On-Demand cached client HTML files do not work with Netscape 6.x or other browsers running with the Java 2 plug-in. You must use the Host On-Demand 7 Deployment Wizard to update these files and select a Java 2 or an Auto Detect client Java type.

Cached client HTML files built with the Host On-Demand 6 Deployment Wizard are compatible with Host On-Demand 7. However, Host On-Demand 6 did not directly support Java 2 for Internet Explorer. If you created your own Host On-Demand 6 Java 2-enabled HTML files, they will not be compatible with Host On-Demand 7. It is recommended that you regenerate all Java 2-enabled Deployment Wizard files with the Host On-Demand 7 Deployment Wizard by selecting a Java 2 or an Auto Detect client Java type.

Java 1 is supported in both Internet Explorer and Netscape 4.x browsers. Java 2 support can be provided for Host On-Demand when running Netscape 6.x, which ships with a Java 2 plug-in, or when running Internet Explorer if a Java 2 plug-in is installed. Host On-Demand provides a Java plug-in that may be used.

If you attempt to use a function of Host On-Demand 7 that requires Java 2, your browser will be checked to determine if a Java 2 plug-in is available:

- If you are running Internet Explorer or Netscape 6.x on a Windows client and a Java 2 plug-in is not found, a window appears asking if you wish to install the Java 2 plug-in that was installed on the Host On-Demand Web server.
- If you are running on any other platform or browser combination, you will be directed to contact your administrator for instructions on installing the Java 2 plug-in. For information on installing Java 2 on non-Windows platforms, see the Sun Microsystems Web site at http://www.javasoft.com.

Certain newer versions of Windows do not ship with Java support. Host On-Demand does not have a way to detect whether Java exists unless Java is already present on the workstation; therefore, your clients will not be directed to the Web page to download and install the Java 2 plug-in. Thus, if you plan to roll out these versions of Windows on your client machines and want to use the Java 2 functions listed above, it is recommended that you install the Java 2 plug-in before rolling out the client machines.

Restricted users do not have the authority to install the Java 2 plug-in. Someone with administrative authority must load the Java 2 plug-in.

If you are using Java 2, the initial startup of Host On-Demand and any sessions may take longer than if you are running Java 1.

If you are a customer who wants to use Host On-Demand 7, but you do not need any of the functions that require Java 2, you will be able to upgrade Host On-Demand, independent of which Java support you have installed. You will have access to all Host On-Demand 7 functions not requiring Java 2.

Accessibility issues

Host On-Demand 7 requires users who want to use accessibility features to have Java 2. To enable accessibility features, you must select Java 2 or Auto Detect in the Deployment Wizard. For more information about accessibility features, see Accessibility in the online help. For more information about Java 2, see "Java 2 upgrade planning issues" on page 23.

Java 2-enabled Web browsers

Host On-Demand 7 clients are supported on Java 2-enabled Web browsers, such as Netscape 6.x and the IBM Web Browser for OS/2. These Web browsers use a Java 2 Runtime Environment (JRE) plug-in that is supplied by Sun Microsystems Inc. or IBM. As newer versions are released, IBM will announce support on the Host On-Demand Web site.

Limitations for Host On-Demand

Java 2 has a stricter security model than older versions of Java, which imposes several restrictions on Host On-Demand:

- Download client limitations: If you are using the Deployment Wizard and select a non-cached Host On-Demand applet with a client java type of Java 2, then the preload component list must be an exhaustive list of what components the client needs because functional components are not downloaded as needed.
- HOD.html limitations: If you use HOD.html to load your download client, you will not be able to use the following functions because they are not part of the initial download:
  - 5250 file transfer
  - Host print sessions
  - Import/export
  - SLP
  - License Use Management (LUM)
  - Thai sessions
  - FTP Codepage Converter
  - Bidirectional sessions
  - 5250 Hindi sessions
  - DBCS sessions using user-defined character settings

  There are three possible solutions to this problem:
  - Use the Deployment Wizard to generate a set of custom HTML files.
  - Use the Host On-Demand cached client for Java 2 browsers.
  - Use the Host On-Demand Download client with Problem Determination. This client includes all of the Host On-Demand classes. The resulting download is 5.5 MB.

- Function On-Demand client (HODThin.html) limitations: The Function On-Demand client will not work with Java 2-enabled Web browsers.

Sun JRE limitations

The Sun JRE has a limitation with Hindi character conversion. To avoid this problem, use the IBM JRE.

Limitations on running applets

If you run applets with your Host On-Demand sessions, permission must be granted by the Java 2 Policy Tool before user-defined applets will run; otherwise, the applet will silently fail.

Limitations on removing the cached client

HODRemove.html cannot remove the cached archive files with Java 2-enabled browsers. The Host On-Demand Java files are stored in the Java Runtime Environment (JRE) cache. The JRE cache is cleared via the JRE Java Control Panel.

- On Windows, start the Java Control Panel by selecting Start > Programs > Java Control Panel or Start > Settings > Control Panel > Java Control Panel.
- When using OS/2, run: `C:\java13\jre\bin\jctrlpnl.cmd`.
- When using Linux and the IBM JRE, run:

  ```
  <JRE install directory>/jre/bin/JavaPluginControlPanel
  ```

  (The install directory is normally /opt/IBMJava 2-13)
-

  When using Linux and the Sun JRE, run:

  ```
  <Java 2 enabled Web browser install directory>/plugins/Java 2/bin/ControlPanel
  ```
- On Solaris, run:

  ```
  <Java 2 enabled Web browser install directory>/java/bin/ControlPanel
  ```

Once the Java plug-in Control Panel is started, click the Cache tab on the top of the window, and then click Clear JAR Cache, which will clear the entire cache, including all applets for all servers.

While using Internet Explorer with Java 1, if you want to remove the cached client, you may experience a problem if a Java 2 plug-in has been installed. The HODRemove file will autodetect Java 2 and will not remove the Java 1 client. Because of this, a link has been added to the HODMain.html file to specifically remove the Java 1 cached client.

Limitations on installing the cached client

With Java 2, the plug-in will cache and manage your Host On-Demand client. If you visit several servers in either your own enterprise, or in multiple enterprises, the plug-in will cache and manage the Host On-Demand client separately for each server. This has several implications:

- Preloading cached clients from a CD or LAN drive serves no function, because when the browser is redirected to the real Web site, the plug-in considers that to be a distinct Web server and the client will be cached again.
- Staging of Host On-Demand updates is managed on a per server basis.

Chapter 5. Planning for security

Whether you are implementing Host On-Demand purely within your corporate network, or you are using it to provide access to your host systems over the Internet, security is a concern. This chapter provides an overview of Host On-Demand security.

- Transport Layer Security (TLS) and Secure Sockets Layer (SSL) security. Provides encryption, certificate-based authentication, and security negotiations over an established Telnet connection. See "TLS and SSL for Host On-Demand" on page 28 for details.
- The Redirector. Supports TLS and SSL between Host On-Demand clients and the Host On-Demand server. See "The Redirector" on page 32 for details.
- Firewalls. You can configure Host On-Demand to go through a firewall. See "Using Host On-Demand with a firewall" on page 33 for details.
- User ID security. Includes Native Authentication and Windows Domain logon. See "User ID security" on page 38 for details.

How TLS and SSL security work

The TLS and SSL security protocols are very similar; in fact, TLS is based on the SSL protocol. TLS differs from SSL mainly in the initial handshake protocol for establishing client/server authentication and encryption. It is also more extensible than SSL. Although they cannot interoperate, TLS provides a mechanism by which a TLS 1.0 implementation can revert to SSL 3.0. For detailed information on TLS, see the description of *The TLS Protocol Version 1.0* at http://www.ietf.org/rfc/rfc2246.txt.

The TLS protocol uses public-key and symmetric-key cryptographic technology. Public-key cryptography uses a pair of keys: a public key and a private key. Information encrypted with one key can be decrypted only with the other key. For example, information encrypted with the public key can be decrypted only with the private key. Each server's public key is published, and the private key is kept secret. To send a secure message to the server, the client encrypts the message by using the server's public key. When the server receives the message, it decrypts the message with its private key.

Symmetric-key cryptography uses the same key to encrypt and decrypt messages. The client randomly generates a symmetric key to be used for encrypting all session data. The key is then encrypted with the server's public key and sent to the server.

TLS provides three basic security services:

Message privacy
Achieved through a combination of public-key and symmetric-key encryption. All traffic between a client and a server is encrypted using a key and an encryption algorithm negotiated during session setup.

Message integrity
Ensures that session traffic does not change en route to its final destination. TLS and SSL use a combination of public/private keys and hash functions to ensure message integrity.

Mutual authentication

Exchange of identification through public-key certificates. The client and server identities are encoded in public-key certificates, which contain the following components:

- Subject’s distinguished name
- Issuer’s distinguished name
- Subject’s public key
- Issuer’s signature
- Validity period
- Serial number

You can also use secure HTTP (HTTPS) to ensure that a client’s security information is not compromised as it is downloaded from a server.

Certificates

Security is controlled by digital certificates that act as electronic ID cards. The purpose of a certificate is to assure a program or a user that it is safe to allow the proposed connection and, if encryption is involved, to provide the necessary encryption/decryption keys. They are usually issued by Certificate Authorities (CAs), which are organizations that are trusted by the industry as a whole and whose business is the issuing of Internet certificates. A CA’s certificate, which is also known as a root certificate, includes (among other things) the CA’s signature and a validity period.

Encryption and authentication are performed by means of a pair of keys, one public, one private. The public key is embedded into a certificate, known as a site or server certificate. The certificate contains several items of information, including the name of the Certificate Authority (CA) that issued the certificate, the name and public key of the server or client, the CA’s signature, and the date and serial number of the certificate. The private key is created when you create a self-signed certificate or a CA certificate request and is used to decrypt messages from clients.

A TLS or SSL session is established in the following sequence:

1. The client and the server exchange hello messages to negotiate the encryption algorithm and hashing function (for message integrity) to be used for the session.
2. The client requests an X.509 certificate from the server to prove its identity. Optionally, the server can request a certificate from the client. Certificates are verified by checking the certificate format and the validity dates and by verifying that the certificate includes the signature of a trusted certificate authority (or is self-signed).
3. The client randomly generates a set of keys that is used for encryption. The keys are encrypted with the server’s public key and securely communicated to the server.

TLS and SSL for Host On-Demand

There are three areas where you can configure security for Host On-Demand: session security, Web server security, and configuration security.

Session security

Host On-Demand can use two protocols to provide security for emulator sessions.

- The TLS protocol provides communications privacy across a TCP/IP network. TLS is designed to prevent eavesdropping, message tampering, or message forgery. TLS also provides a framework that allows new cryptographic algorithms to be easily incorporated. Host On-Demand supports encryption of emulation sessions and server/client authentication according to *TLS Protocol Version 1.0* standard (available at http://www.ietf.org/rfc/rfc2246.txt). TLS is the default security protocol for emulator sessions when security is enabled.
- The SSL protocol provides encryption and authentication on connections across a TCP/IP network, using X.509 certificates. Host On-Demand supports encryption of emulation sessions and server/client authentication according to the SSL Version 3.0 standard.

Support is provided for the following:

- RSA type-4 data encryption on connections between the Host On-Demand emulators and Telnet servers that support TLS version 1.0 and SSL version 3
- X.509 certificates
- Bulk encryption algorithms using keys up to 168 bits in length
- Authentication algorithms using keys up to 1024 bits in length
- Server and client authentication
- Support for storage and use of client certificates on the client system
- Optional prompting of user for client certificate when requested by server

For Host On-Demand, you can use a CA's certificate, but you can also create your own self-signed certificate, as described in the Using a self-signed certificate topic in the online help.

A Certificate Wizard (available on Windows platforms) and a graphical Certificate Management utility (available on Windows and AIX platforms) are provided to:

- Create certificate requests
- Receive and store certificates
- Create self-signed certificates

IKEYCMD is a tool, in addition to the Certificate Management Utility, that can be used to manage keys, certificates, and certificate requests. IKEYCMD is functionally similar to Certificate Management and is meant to be run from the command line without a graphical interface. For more information, refer to Appendix C, "Using the IKEYCMD command-line interface" on page 137.

To support TLS and SSL services, Host On-Demand uses three databases:

HODServerKeyDb.kdb
The HODServerKeyDb.kdb is created the first time you configure TLS or SSL for the Host On-Demand Redirector. This database contains the server's private key and certificate, and a list of CA (or signer) certificates. These CAs are considered *well-known* and are *trusted* by the Host On-Demand server. You can add certificates from other CAs (unknown CAs) and certificates that you create and sign yourself (self-signed) to this database. See "The Redirector" on page 32 for more information.

CustomizedCAs.class
The CustomizedCAs.class is a Java class file that contains the certificates of unknown CAs and self-signed certificates that are not in the

WellKnownTrusted list. If you use a self-signed certificate or a certificate from an unknown authority (CA), you must create or update the CustomizedCAs.class. Host On-Demand does not install a CustomizedCAs.class file by default.

WellKnownTrustedCAs.class
The WellKnownTrustedCAs.class is a Java class file supplied by Host On-Demand that contains the public certificates of all the CAs that Host On-Demand trusts. You should not modify this file.

Both WellKnownTrustedCAs.class and CustomizedCAs.class must be present in the Host On-Demand publish directory. The Host On-Demand client uses these two classes to trust the Server's certificate during the TLS or SSL handshake.

Basic TLS or SSL enablement for Host On-Demand clients

By default, when security is enabled for the Host On-Demand client, a basic TLS or SSL session is established. During the TLS or SSL negotiation process, the server presents its certificate to the client. With basic TLS or SSL enablement, the certificate must be signed by an authority that the client trusts. The client checks WellKnownTrustedCAs.class first, followed by the CustomizedCAs.class. The client rejects the session if it does not find the signer in these files. If the client finds the signer in these files, the session is established. This is basic Server Authentication. Host On-Demand allows you to configure a more enhanced form of Server Authentication in its client configuration. Refer to the following section for more information.

Server authentication
Encrypting the data exchange between the client and the server does not guarantee the client is communicating with the correct server. To help avoid this danger, you can enable server authentication, so that 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 TLS or SSL negotiation will continue. If not, the connection ends immediately. See server authentication in the Host On-Demand online help for more information.

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. Not all servers support client authentication, including the Host On-Demand Redirector. To configure client authentication, you must: obtain certificates for clients; send the certificates to the clients; and configure the clients to use client authentication. See configuring clients to use client authentication in the Host On-Demand online help for more information.

Express logon
You can provide users with an easy host logon process by creating a macro to allow a user to log on without having to enter a user ID and password . Using this function reduces the time spent by an administrator maintaining host user IDs and passwords. To use Express Logon, the session must be configured for TLS or SSL and client authentication, and the Communications Server must support and be configured for Express Logon. See Express logon in the Host On-Demand online help for more information.

TLS-based Telnet Security
Telnet-negotiated security allows the security negotiations between the client and the Telnet server to be done on the established Telnet

connection. You can configure Telnet-negotiated security for Host On-Demand 3270 display and printer sessions.

The Telnet server must support TLS-based Telnet security (as described in the IETF Internet-Draft *TLS-based Telnet Security*, available at http://www.ietf.org/internet-drafts/draft-ietf-tn3270e-telnet-tls-06.txt) for the Host On-Demand clients to use Telnet-negotiated security. The Communications Server for OS/390 Version 2 Release 10 and later supports TLS-based Telnet security. Communications Server for OS/390 documentation refers to Telnet-negotiated security as ″negotiable SSL.″

For more information regarding Telnet-negotiated security, see the Telnet-negotiated security overview in the Host On-Demand online help. See your Telnet server's documentation for more information about configuring TLS or SSL on the Telnet server, and see the Security topic in the Host On-Demand online help for more information about configuring a client to connect to a secure Telnet server.

Examples of when to use session security

Some situations where you might want to use session security include:

- You want to let customers order your products over the Internet. You want to make sure information they give you, such as a credit-card number, is encrypted so that it cannot be stolen. You also want to make sure information you give to customers is protected.
- You want to give your suppliers or business partners access to certain information on your host computers and to be sure that the data is not available to anyone else.
- You want your staff to have access to your host-computer information from remote sites or when they are traveling.
- You are a hospital administrator and want doctors to have access to patient records from wherever they are and to be sure that the records cannot be seen by unauthorized people.

Web server security

You can configure your Web server to use TLS or SSL (HTTPS), so that the data stream from your Web server to your browser is encrypted. See your Web server documentation for more information about configuring your Web server for TLS or SSL. Once the client is loaded in a browser, however, it communicates directly with the host. You can configure Host On-Demand to provide TLS or SSL security to your host sessions. For more information, see Configuring TLS and SSL in the online help.

Configuration security

If you use the HTML model, your session configuration information will be encrypted if you use HTTPS. For all other models, you need to configure Host On-Demand to use the configuration servlet over HTTPS (after configuring your Web application server) to encrypt the session configuration instead of communicating directly with the configuration server. See "Installing the configuration servlet" on page 59 in this guide for more information about installing the configuration servlet, and see configuring the configuration servlet in the Host On-Demand online help for more information about configuring clients to use the configuration servlet.

The Redirector

Why use the Redirector?

If your Telnet server does not support TLS or SSL, and you are running Host On-Demand on Windows NT, Windows 2000, or AIX on Netscape Communicator 4 or Internet Explorer 4 or later browsers, you can configure the Host On-Demand Redirector to provide TLS or SSL support. The Redirector, which resides on the Host On-Demand Server, provides support for TLS and SSL security between clients and the Host On-Demand server.

Many Telnet servers support TLS or SSL (for example, IBM Communications Servers on zSeries, iSeries, AIX, NT, and OS/2). If your Telnet server supports TLS or SSL, we strongly recommend using your Telnet server. If your Telnet server does not support TLS or SSL, the Communications Server for AIX Redirector offers a more scalable alternative to the Host On-Demand Redirector.

The Redirector acts as a transparent Telnet proxy that uses port remapping to connect the Host On-Demand server to other Telnet servers. Each defined server can configure a set of local-port numbers. Instead of connecting directly to the target Telnet server, a client connects to the Host On-Demand server and port number. The Redirector maps the local-port number to the host-port number of the target and makes a connection.

The recommended solution for a Telnet proxy is to use Load Balancer, a feature of WebSphere Application Server's Edge Components, or a similar product that provides address translation as part of the overall firewall solution, instead of the Host On-Demand Redirector.

How the Redirector works

The following scenario shows how the Redirector works.

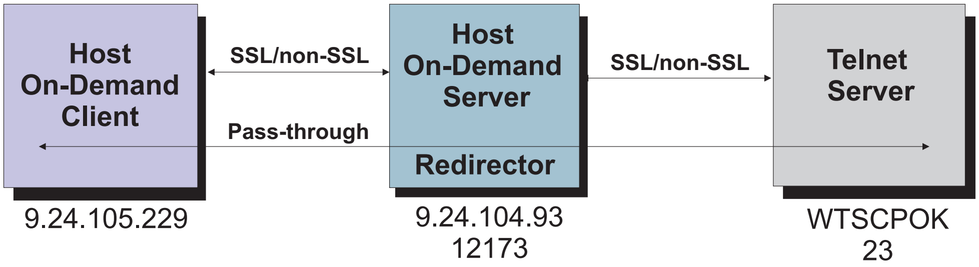

Figure 5. How the Redirector works

For each port configured on the Redirector, an administrator has the following security options:

- Pass-through - data between the client and the host is not altered
- Client side - encrypts data between the client and the redirector
- Host side - encrypts data between the redirector and the host
- Both - does client-side and host-side security

You must create the HODServerKeyDb.kdb for the Redirector before you can enable client-side security, server-side security, or both.

You can use pass-through when encryption by the Redirector is not necessary, either because the data-stream does not need to be encrypted, or because the data-stream is already encrypted between the client and the host. You must use pass-through if the Host On-Demand client is connecting through the Redirector to a host that requires client authentication or Express Logon.

See adding a host to the Redirector in the Host On-Demand online help for more information.

Using Host On-Demand with a firewall

If you are configuring Host On-Demand to go through a firewall, it is recommended that the firewall administrator open only those ports required for the clients to function. Telnet ports allow TLS or SSL-encrypted session traffic.

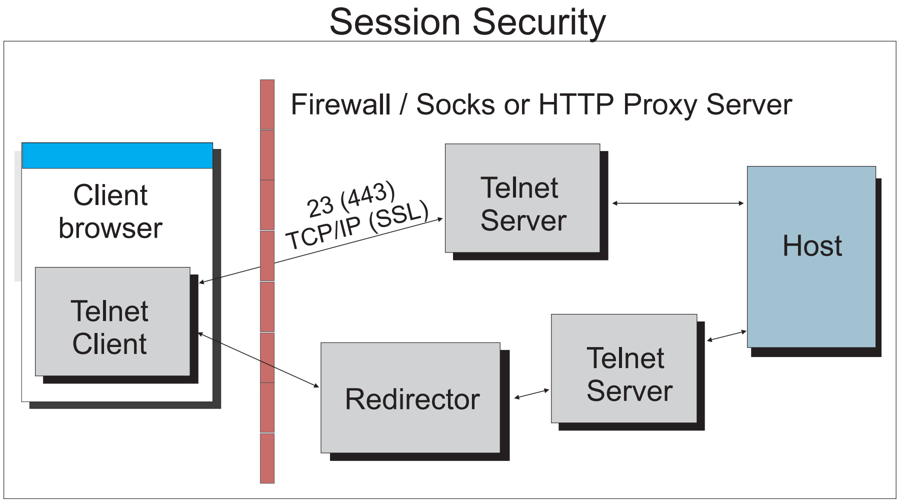

Figure 6. Session security through a firewall or proxy server

The Host On-Demand configuration servlet allows Host On-Demand clients to communicate with the configuration server across either HTTP or HTTPS.

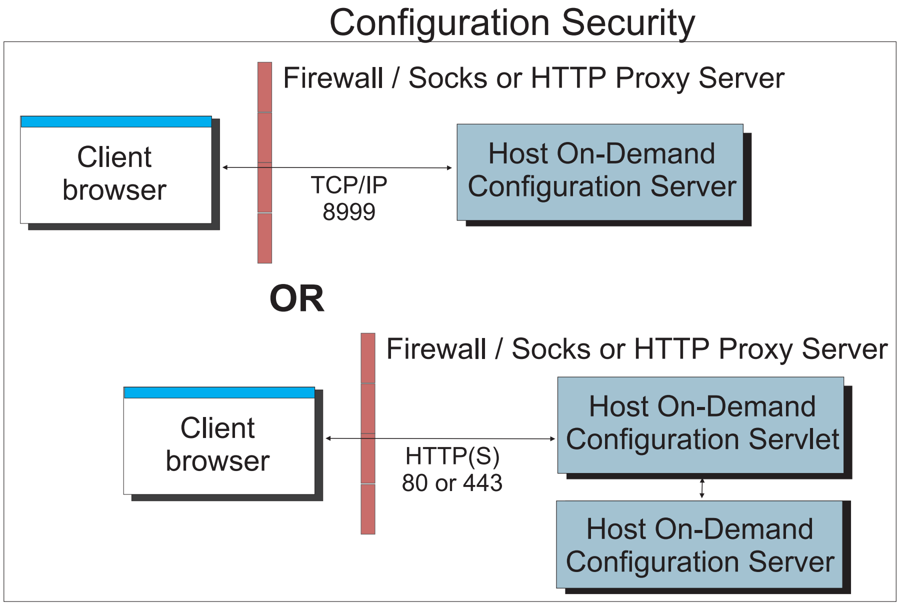
Configuration Security
Firewall / Socks or HTTP Proxy Server
Client browser
TCP/IP 8999
Host On-Demand Configuration Server
OR
Firewall / Socks or HTTP Proxy Server
Client browser
HTTP(S) 80 or 443
Host On-Demand Configuration Servlet
Host On-Demand Configuration Server

Figure 7. Configuration security with and without the configuration servlet through a firewall or proxy server

Host On-Demand clients connecting to a host system through open ports in the firewall should see "Configuring firewall ports" for details. Host On-Demand clients connecting to a host system through a Socks or HTTP proxy server should see "Connecting to a host system through a proxy server" on page 36 for details.

Configuring firewall ports

If you are using the configuration server based model or the combined model, your Host On-Demand clients will need to communicate with the configuration server. To allow this through a firewall, you will need to either open the Host On-Demand Service Manager port or use the Host On-Demand configuration servlet. The Service Manager listens on port 8999 by default. You can change this default to any other available port number. For details, see Changing the Service Manager port in the Host On-Demand online help. The Host On-Demand configuration servlet allows Host On-Demand clients to communicate with the configuration server across either HTTP or HTTPS. Therefore, the Service Manager port does not need to be open on the firewall. (See Figure 4 on page 21.) See "Installing the configuration servlet" on page 59 and Configuring the configuration servlet in the online help for details on using the configuration servlet.

If you are using the HTML-based model, there is no requirement for Host On-Demand clients to access the configuration server, and the Service Manager port does not need to be open on the firewall. The clients will still attempt to contact the configuration server for license counting but will fail silently if the Service Manager port is not open. If you want to prevent clients from making license counting requests, you can add a parameter Disable with a value of LUM in the Additional Parameters tab on the Advanced Options window in the Deployment Wizard.

In addition to the Service Manager port, make sure the firewall administrator opens any ports that are being used for functions your clients use. For example, if you have a TLS or SSL session with the Redirector on port 5000, port 5000 must be open for Telnet traffic. The following table summarizes the ports that Host On-Demand can use.

Table 10. Host On-Demand functions and the ports they use

Host On-Demand Function	**Ports Used**
Display emulation (3270 and VT) and 3270 Printer emulation	23 (Telnet), 80 (HTTP), or 443 (TLS or SSL) and 8999 (config server)[3]
5250 Display and Printer emulation	23 (Telnet) or 992 [1] (TLS or SSL) or 80 (HTTP) or 443 (TLS or SSL) and 8999 (config server) [3]
3270 file transfer	23 (Telnet), 80 (HTTP), or 443 (TLS or SSL) and 8999 (config server)[3]
5250 file transfer - savfile	80 (HTTP), 8999 (config server)[3], 21 (FTP)[4], >1024 (FTP)[4], 446 (drda)[4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], 8475 (as-rmtcmd)[1 4], and 8476 (as-signon)[1 4]
5250 file transfer - database	80 (HTTP), 8999 (config server)[3], 446 (drda)[4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], 8475 (as-rmtcmd)[1 4], and 8476 (as-signon)[1 4]
5250 file transfer - stream file	80 (HTTP), 8999 (config server)[1 2 4], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8473 (as-file)[1 4], and 8476 (as-signon)[1 4]
FTP	21 (FTP), 80 (HTTP), 8999 (config server)[1 2 4], and >1024 (FTP)[5]
CICS	2006
Database On-Demand	80 (HTTP), 8999 (config server)[3], 449 (as-svrmap)[4], 8470 (as-central)[1 2 4], 8471 (as-database)[1 4], and 8476 (as-signon)[1 4]
License Use Management (LUM)	8999 (config server) for default licence use counting using the configuration server, 80 (HTTP) for license use counting using a License Use Management Server
Host On-Demand clients	23 (Telnet), 80 (HTTP), and 8999 (config server)[3]
Administration clients	80 (HTTP) and 8999 (config server)[3]

Notes:

1 You can change the port numbers with the command `WRKSRVTBLE` . The port numbers listed are the default values.

2 The port for as-central is used only if a codepage conversion table needs to be created dynamically (EBCDIC to/from Unicode). This is dependant on the JVM and the locale of the client.

3 You can change the config server port. Port 8999 is the default.

4 These ports do not need to be opened on the firewall if you are using iSeries proxy server support. You will need to open the default proxy server port 3470. You can change this port.

5 In passive (PASV) mode, the FTP client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening a FTP connection, the client opens two random unprivileged ports locally (N>1024 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client issues the PASV command. As a result, the server then opens a random unprivileged port (P>1024) and sends the PORT P command back to the client. The client then initiates the connection from port N+1 to port P on the server to transfer data.

From the server-side firewall's standpoint, to support passive mode FTP, you must open the following communications ports:

- FTP server's port 21 from anywhere (client initiates connection)
- FTP server's port 21 to remote ports >1024 (server responds to client's control port)
- FTP server's ports >1024 from anywhere (client initiates data connection to random port specified by server)
- FTP server's ports >1024 to remote ports >1024 (server sends ACKs (and data) to client's data port)

If you do not want to open port 8999 on the firewall, you can still allow users to access Host On-Demand. There are two options:

- Use the Deployment Wizard to create HTML files that contain all configuration information. This eliminates the need to access the configuration server. When creating the HTML files, choose "HTML-based model" from the Configuration Model page of the Deployment Wizard.
- If you want to use the configuration server, you can configure clients to use the configuration servlet. See Configuring the configuration servlet in the Host On-Demand online help. This option is only available if your Web server supports servlets.

  If you use the configuration server and it is separated from your Web browser by a firewall, you will either need to open the configuration server port on the firewall or run the Host On-Demand configuration servlet. The configuration servlet allows the browser to communicate with the configuration server across standard Web protocols, such as HTTP or HTTPS. (See Figure 4 on page 21.)

Connecting to a host system through a proxy server

Host On-Demand clients can use a proxy server to transparently access host systems from behind a firewall. Two types of proxy servers are supported:

- Socks proxy servers, described in "Connecting through a Socks proxy server" on page 37. Both version 4 and version 5 of Socks are supported.
- HTTP proxy servers, described in "Connecting through an HTTP proxy server" on page 37.

Before you can connect to a host system through a proxy server, you must find out which protocol the proxy server supports. Decide whether you want to specify the proxy server settings through the Web browser or explicitly identify a proxy server for the session. If you decide to explicitly identify a proxy server, you must specify the protocol that the proxy server uses, the proxy server name and port number, and other information.

In general, if a Socks proxy server is available, configure Host On-Demand sessions to use it. Configure sessions to use an HTTP proxy server if that is the only type of proxy server supported at your site.

Connecting through a Socks proxy server

Many organizations use Socks proxy servers to protect computing resources behind a firewall. Socks is a protocol for TCP/IP-based network proxies. It allows applications on one side of a Socks proxy server to gain full access to hosts on the other side of the Socks proxy server without directly connecting to them. Proxy servers are generally used in conjunction with firewalls. Under the Socks protocol, a client that requests a connection to a host system through a firewall actually connects to a Socks proxy server. The Socks proxy server acts as an intermediary between the client and the host system. It authorizes communication requests, connects to the host on behalf of the client, and relays data between the two systems.

Host On-Demand supports both version 4 and version 5 of the Socks protocol.

- Socks version 4 specifies the message format and conventions to allow TCP-based application users access across a firewall. It provides access control based on TCP header information, including IP addresses and source and destination port numbers.
- Socks version 5 (also known as authenticated firewall traversal (AFT)) is an open Internet standard for network proxies. It adds authentication, better support for resolving domain names, support for IP version 6 addresses, and other features to version 4. These features are very useful for clients located outside a firewall. A Socks user ID and password for the proxy server can optionally be sent over the connection between the Host On-Demand client and the proxy server. The user ID and password are not encrypted. For more information on version 5, see *Socks Protocol Version 5* (RFC 1928), available at http://www.ietf.org/rfc/rfc1928.txt?number=1928.

The Java virtual machine (JVM) used in most Web browsers supports Socks version 4. A session can access either a Socks version 4 or version 5 proxy server, bypassing the proxy server settings in the Web browser. You can also have the session negotiate a Socks version 4 connection if the proxy server does not support version 5. For more information on Socks proxy server settings, see the Proxy Server tab topic in the online help.

Connecting through an HTTP proxy server

HTTP proxy servers are used to handle HTTP requests through firewalls. They act as intermediaries between private local networks and the Internet. The HTTP proxy server is connected to both the local network and the Internet. Local users configure their browsers to pass HTTP requests through the HTTP proxy server by specifying the proxy server’s IP address and TCP port number. The HTTP proxy server accepts these HTTP requests and forwards them to the actual Web servers specified by the URLs entered in the browser.

For Host On-Demand clients, HTTP proxy servers act as forwarding agents for connections to a host system. The HTTP proxy server opens a connection to the host system and sends data back and forth between the host system and the client. Although an HTTP proxy server usually closes a connection after servicing an HTTP request, Host On-Demand keeps the connection open for host traffic by using the HTTP Connect method (if it is enabled for the proxy server).

To have a session use an HTTP proxy server, you need to select HTTP proxy as the protocol and specify the proxy server name and port number. For more information on HTTP proxy server settings, see the Proxy Server tab topic in the online help.

User ID security

Native Authentication

If you use the configuration server-based model, you can configure your Host On-Demand users to be natively authenticated. This option allows users to log on to Host On-Demand using the same password as they would to log on to the operating system (Windows NT, AIX, or z/OS) where Host On-Demand is active. When a user logs on to Host On-Demand, their password is validated against the operating 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.

See Native Authentication in the online help for more information on enabling this option.

Windows Domain logon

If your users are logged on to a Windows domain, this option (available with the configuration server-based model in the Deployment Wizard) automatically logs users on to Host On-Demand using their Windows user name. The Host On-Demand logon window does not appear and the Windows user name is used as the Host On-Demand user ID. If a Host On-Demand user ID does not already exist (matching the Windows user name), you can also choose to have a user ID automatically created in the specified Host On-Demand group.

See Logon Type in the online help for more information on choosing how users access the Host On-Demand configuration server.

Chapter 6. Planning for national language support

Host On-Demand is provided in 23 languages. The session windows, configuration panels, help files, and the documentation have been translated. In addition, display, keyboard, and processing support is provided for Arabic, Hebrew, Thai, and Hindi. This support is fully explained in the online help.

All the translated versions are provided on the CDs and on the zSeries tapes. When you install Host On-Demand on Windows platforms or AIX using the graphical installation program, you can choose which languages to install. On the other operating systems, all the languages are always installed.

National language support is operating-system dependent, so the appropriate font and keyboard support for the language you want to use must be installed in the operating system. For example, if you want to use French as the host-session language but do not have the French font and keyboard support installed, you may not be able to display the correct characters.

DBCS cannot be used as the HTML file name.

Supported languages

The languages into which Host On-Demand has been translated are listed below, along with the language suffixes you can use to load translated versions of the Host On-Demand clients. For example, IBM-supplied HTML pages have language extensions to identify different language installations and different language predefined HTML files.

Language	Language suffix
Simplified Chinese	zh
Traditional Chinese	zh_TW
Czech	cs
Danish	da
Dutch	nl
English	en
Finnish	fi
French	fr
German	de
Greek	el
Hungarian	hu
Italian	it
Japanese	ja
Korean	ko
Norwegian	no
Polish	pl

Brazilian Portuguese	pt
Portuguese	pt_PT
Russian	ru
Slovenian	sl
Spanish	es
Swedish	sv
Turkish	tr

Supported host code pages

Host On-Demand supports multiple code pages. You can specify these code pages on a session-by-session basis.

3270 and 5250 code pages

The code pages specified below are supported by the 3270 and 5250 emulators. You can select them in the Session Configuration window.

Country or region	Code page	Note
Arabic Speaking	420	
Austria	273	
Austria (Euro)	1141	
Belarus	1025	
Belarus (Euro)	1154	
Belgium	037	
Belgium (Euro)	1140	
Belgium (Old Code)	274	
Bosnia/Herzegovina	870	
Bosnia/Herzegovina (Euro)	1153	
Brazil	037	
Brazil (Euro)	1140	
Brazil (Old)	275	
Bulgaria	1025	
Bulgaria (Euro)	1154	
Canada	037	
Canada (Euro)	1140	
China (Simplified Chinese Extended)	1388	
Croatia	870	
Croatia (Euro)	1153	
Czech Republic	870	
Czech Republic (Euro)	1153	
Denmark	277	
Denmark (Euro)	1142	
Estonia	1122	

Estonia (Euro)	1157	
Finland	278	
Finland (Euro)	1143	
France	297	
France (Euro)	1147	
FYR Macedonia	1025	
FYR Macedonia (Euro)	1154	
Germany	273	
Germany (Euro)	1141	
Greece	875	
Hebrew (New Code)	424	
Hebrew (Old Code)	803	
Hindi	1137	5250 display only
Hungary	870	
Hungary (Euro)	1153	
Iceland	871	
Iceland (Euro)	1149	
Italy	280	
Italy (Euro)	1144	
Japan (Katakana)	930	
Japan (Katakana Extended)	930	
Japan (Katakana Unicode Extended)	1390	3270 only
Japan (Latin Extended)	939	
Japan (Latin Unicode Extended)	1399	
Korea (Euro)	1364	
Korea (Extended)	933	
Latin America	284	
Latin America (Euro)	1145	
Latvia	1112	
Latvia (Euro)	1156	
Lithuania	1112	
Lithuania (Euro)	1156	
Multilingual	500	
Multilingual ISO (Euro)	924	
Multilingual (Euro)	1148	
Netherlands	037	
Netherlands (Euro)	1140	
Norway	277	
Norway (Euro)	1142	
Open Edition	1047	

Poland	870	
Poland (Euro)	1153	
Portugal	037	
Portugal (Euro)	1140	
Romania	870	
Romania (Euro)	1153	
Russia	1025	
Russia (Euro)	1154	
Serbia/Montenegro (Cyrillic)	1025	
Serbia/Montenegro (Cyrillic; Euro)	1154	
Slovakia	870	
Slovakia (Euro)	1153	
Slovenia	870	
Slovenia (Euro)	1153	
Spain	284	
Spain (Euro)	1145	
Sweden	278	
Sweden (Euro)	1143	
Taiwan (Traditional Chinese Extended)	937	
Taiwan (Traditional Chinese Extended; Euro)	1371	
Thai	838	
Thai (Euro)	1160	
Turkey	1026	
Turkey (Euro)	1155	
Ukraine	1123	
Ukraine (Euro)	1158	
United Kingdom	285	
United Kingdom (Euro)	1146	
United States	037	
United States (Euro)	1140	

Notes:

- 3270 host print with a Printer Definition Table (PDT) supports only Latin-1, DBCS, bidirectional, and Thai code pages. Other code pages are supported either in Adobe PDF printing or on Windows platforms without a PDT.
- In order to include more characters (which are defined in the GB18030 standard by the Government of the People's Republic of China), 6582 Unicode Extension-A and 1,948 additional non-Han characters (Mongolian, Uygur, Tibetan, and Yi) were added to the Simplified Chinese code page 1388 for Host On-Demand Version 6.

VT code pages

Language	Code page
Arabic	ASMO 708 and ASMO 449
British	1101
DEC Greek	
DEC Hebrew	
DEC Multinational Replacement Character Set	1100
DEC Technical	
Dutch	1102
Finnish	1103
French	1104
French Canadian	1020
German	1011
Hebrew NRCS	
ISO Greek Supplemental (ISO Latin-7)	813
ISO Hebrew Supplemental	
ISO Latin-1	819
Italian	1012
Norwegian/Danish	1105
PC Danish/Norwegian	865
PC International	437
PC Multilingual	850
PC Portugese	860
PC Spanish	220
Spanish	1023
Swedish	1106
Swiss	1021
United States	1100

CICS Gateway code pages

Code page	Character set
000	Auto-Detect (default)
437	Latin-1
813	ISO Greek (8859_7)
819	ISO Latin 1 (8859_1)
850	Latin 1
852	Latin 2
855	Cyrillic
856	Hebrew
857	Latin 5

864	Arabic
866	Cyrillic
869	Greek
874	Thai
912	ISO Latin 2 (8859_2)
915	ISO Cyrillic (8859_5)
920	ISO Latin 5 (8859_9)

User-defined character mapping

For double-byte character set (DBCS) languages, you can use customized user-defined character (UDC) mapping in your session (3270, 5250, 3270 host print) instead default mapping. You can create a UDC translation table using the UDC mapping editor to store customized mapping for your session. For instructions for how to use the UDC mapping editor to change your character mapping, see Using the user-defined character (UDC) mapping editor in the online help.

Part 2. Installing, upgrading, and uninstalling Host On-Demand

Chapter 7. Installing the Host On-Demand server and related software

Three different Host On-Demand components can be installed:

- The Host On-Demand server, which is necessary for using Host On-Demand. See “Installing the Host On-Demand server” for instructions.
- The Host On-Demand configuration servlet, which is needed only if you plan to use Host On-Demand with a Web application server. See “Installing the configuration servlet” on page 59 for instructions.
- The Deployment Wizard, an extremely useful tool that runs on Windows, generates customized Host On-Demand clients. Installing the Deployment Wizard is not required, but it is highly recommended. See “Installing the Deployment Wizard” on page 61 for instructions.

If you are upgrading from an earlier version of Host On-Demand, see Chapter 8, “Upgrading from earlier versions of Host On-Demand” on page 63 for instructions on how to successfully upgrade your system.

Installing the Host On-Demand server

To install the Host On-Demand server, follow the instructions for the desired platform.

- “Installing on zSeries”
- “Installing on iSeries”
- “Installing on Windows platforms” on page 51
- “Installing on AIX” on page 54
- “Installing on the Solaris, HP-UX, and Linux platforms” on page 56
- “Installing on OS/2” on page 57
- “Installing on Novell NetWare” on page 58

Host On-Demand clients are served as Web pages, so you must install the Host On-Demand server in the same environment as a Web server.

Installing on zSeries

For instructions about installing Host On-Demand on z/OS, refer to the program directory supplied with the z/OS or legacy OS/390 program product.

For instructions on installing Host On-Demand on Linux/390, see “Installing on the Solaris, HP-UX, and Linux platforms” on page 56.

For information on configuring Host On-Demand on zSeries, see Chapter 15, “Configuring Host On-Demand on zSeries” on page 105.

Installing on iSeries

Installing Host On-Demand on iSeries is a two step process:

1. Install the Host On-Demand server software.
2. Configure the HTTP server.

After completing the installation process, see “Configuring, starting, and stopping the Host On-Demand Service Manager on iSeries” on page 115 for instructions on configuring the Service Manager.

For information on configuring Host On-Demand on iSeries, see Chapter 16, “Configuring Host On-Demand on iSeries” on page 115.

Install the software

1. Sign on to the iSeries with the QSECOFR user profile (or user profile with equivalent security authorities).
2. If Host On-Demand has previously been installed, issue the following OS/400 command to shutdown the Service Manager:

   ```
   ENDHODSVM
   ```

3. If you previously installed Host On-Demand, do the following:
   a. Type the following command to migrate the NSMprop file to the correct location for Host On-Demand 7:

      ```
      MOV OBJ('/QIBM/ProdData/hostondemand/lib/NSMprop')
           TODIR('/QIBM/ProdData/hostondemand/private')
      ```

   b. Type the following commands to back up the current settings:

      ```
      CRTSAVF QGPL/HOD
      CALL QCMD
      ```

   c. Press the F11 key and enter the following command on line 2 of the window:

      ```
      SAV DEV('/qsys.lib/qgpl.lib/hod.file')
        OBJ(('/qibm/proddata/hostondemand/private/*')
        ('/QIBM/ProdData/hostondemand/hod/*.html')
        ('/QIBM/ProdData/hostondemand/hod/hoddata/*')
        ('/QIBM/ProdData/hostondemand/hod/custom/*')
        ('/QIBM/ProdData/hostondemand/hod/config.properties')
        ('/QIBM/ProdData/hostondemand/hod/CustomizedCAs.class')
        ('/QIBM/ProdData/hostondemand/lib/com/ibm/as400/access/keyring.class'))
      ```

   The line beginning with SAV and ending with keyring.class')) should be one line on your command line.

   One or more "Object not found" (CPFA0A9) messages may appear if the config.properties or hoddata files are not on your system.

4. Place the Host On-Demand for OS/400 CD in the iSeries CD drive.
5. Type the following OS/400 command:

   ```
   RSTLICPGM LICPGM(5733A59) DEV(OPT01)
   ```

   This command will process for 10-45 minutes, depending upon the configuration of the iSeries.

6. For each additional OS/400 secondary language that you would like to provide full help text support for, type the following OS/400 command:

   ```
   RSTLICPGM LICPGM(5733A59) DEV(OPT01) LNG(xxxx) RSTOBJ(*LNG)
   ```

   Where *xxxx* is the language code from the list below. This step is optional and can be performed after installation.

Language	Language code
Belgian Dutch	2963
Belgian English	2909

Belgian French	2966
Brazilian Portuguese	2980
Canadian French	2981
Chinese (simplified) PRC	2989
Chinese (traditional) Taiwan	2987
Czech	2975
Danish	2926
Dutch Netherlands	2923
English	2924
English DBCS (uppercase)	2938
English (uppercase)	2950
English DBCS	2984
Finnish	2925
French	2928
French Multinational	2940
German	2929
German Multinational	2939
Greek	2957
Hungarian	2976
Italian	2932
Italian Multinational	2942
Japanese Kanji DBCS	2962
Korean DBCS	2986
Norwegian	2933
Polish	2978
Portuguese	2922
Portuguese Multinational	2996
Russian	2979
Slovenian	2911
Spanish	2931
Swedish	2937
Thai	2972
Turkish	2956

7. Install IBM Screen Customizer 2.0.70 for iSeries (if you are planning to use the full runtime features). If you have previously installed IBM Screen Customizer, you must install the new version at this time. Refer to the installation manual for Screen Customizer.
8. If you want the Host On-Demand Service Manager to automatically start after an IPL (when QSYSWRK is started), type the following OS/400 command:

   ```
   CFGHODSVM AUTOSTART(*YES)
   ```
9. To restore the former configuration settings (if Host On-Demand was previously installed), do the following:
   a. Enter the following command:

```
CALL QCMD
```

b. Press the F11 key and enter the following command in line 2 of the window:

```
RST DEV('/qsys.lib/qgpl.lib/hod.file')
  OBJ(('/qibm/proddata/hostondemand/private/*')
  ('/QIBM/ProdData/hostondemand/hod/config.properties')
  ('/QIBM/ProdData/hostondemand/hod/hoddata/*')
  ('/QIBM/ProdData/hostondemand/hod/custom/*')
  ('/QIBM/ProdData/hostondemand/hod/config.properties')
  ('/QIBM/ProdData/hostondemand/hod/CustomizedCAs.class')
  ('/QIBM/ProdData/hostondemand/lib/com/ibm/as400/access/keyring.class'))
  OUTPUT(*PRINT) ALWOBJDIF(*ALL)
```

The line beginning with `RST` and ending with `ALWOBJDIF(*ALL)` should be one line on your command line.

One or more messages may appear if config.properties is not on your system.

10. To restore custom built web pages in the Host On-Demand publish directory, enter the following command:

```
RST DEV('/qsys.lib/qgpl.lib/hod.file')
OBJ(('/qibm/proddata/hostondemand/hod/*.html')
OUTPUT(*PRINT)
```

By not specifying `ALWOBJDIF(*YES)`, this step avoids replacing *.html objects that are part of Host On-Demand .

Configure the iSeries HTTP server

For Apache and Lotus Notes HTTP server configuration, refer to Section 4 of the *IBM Host Access Client Package* Redbook (part number SG24-6182).

The following commands assume that you are using the IBM HTTP server's `DEFAULT HTTP` configuration and `CONFIG HTTP` instance. These adjustments are necessary to grant the HTTP server permission to serve objects from the `/qibm/proddata/hostondemand/hod` directory. For more information, refer to the iSeries Webmaster's Guide at the following site:

`http://publib.boulder.ibm.com/html/as400/`

`v5r1/ic2924/info/rzahl/rzahlusergoal.htm`

1. Stop the Web server using the following command:

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

2. Configure the Web server using the following command:

   ```
   WRKHTTPCFG
   ```

3. Make sure that active `Enable POST` and `Enable GET` entries exist and are not commented out. Add the following entry (there must be one space before the first slash (/) and after the first asterisk (*)):

   ```
   pass /hod/* /QIBM/ProdData/hostondemand/HOD/*
   ```

   This entry creates an alias, `hod` , for the path to the Host On-Demand files. You must type it exactly as you typed the original directory names, matching upper and lower case.

4. Press F3 to exit the `WRKHTTPCFG` tool.

5. Start the Web server using the following command:

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

6. If you want the Web server to automatically start after an IPL (when QSYSWRK is started), type the following command:

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

7. Load http://*server_name*/hod/hodmain.html (where *server_name* is the name of your server) to verify that the Web server can serve Host On-Demand HTML files.

After you set up the HTTP server, see “Configuring, starting, and stopping the Host On-Demand Service Manager on iSeries” on page 115 for instructions on configuring the Service Manager.

Installing on Windows platforms

A Web server is required to install Host On-Demand on Windows NT, Windows 2000, or Windows XP. See Chapter 2, “Requirements” on page 13 for a list of supported Web servers.

You can install Host On-Demand with a graphical interface using Windows InstallShield or with a response file using Windows InstallShield in silent mode.

The Host On-Demand InstallShield does not support accessibility features.

Installing the Host On-Demand server using InstallShield

To automatically install the Host On-Demand server on a Windows NT, Windows 2000, or Windows XP workstation using InstallShield, follow the steps below.

1. Log in as Administrator or a user that is a member of the Administrators group.
2. If CD autoplay is enabled on your Windows NT, Windows 2000, or Windows XP server, insert the CD and wait for the start window. Otherwise, insert the CD and run the `setupwin.exe` program in the root directory.
3. Click Install Product.
4. Follow the directions in the installation windows.
   - The default server directory is `hostondemand` . If you are upgrading, the installation program uses the same server directory as before. The server directory contains files used only by the server and must not be available to client workstations.
   - The default publish directory is `\hostondemand\HOD`. The publish directory contains files that must be available to client users who access the server through a browser.
   - The default Service Manager port is 8999, and it is usually a safe port to select. Check your server documentation to see if this port is being used. If it is in use, you can change the port during installation, or later. For more information about changing the Service Manager port, see Changing the Service Manager’s configuration port in the online help.
   - If the installation program detects that IBM WebSphere Application Server is installed, you are asked if you want to use the configuration servlet to connect to the configuration server for client configuration information. If you are running Host On-Demand through a firewall, this eliminates the need to open an extra port for the configuration server. Answering Yes automatically configures the clients to access the configuration server through the configuration servlet. Answering No configures the clients to access the configuration server directly on port 8999. See “Installing the configuration servlet” on page 59 for more information.

5. A window appears giving you the option to register your software and view the *Planning, Installing, and Configuring Host On-Demand* guide.
6. If a message tells you that your Web server is not recognized or was not configured, configure it. If you install a Web server later or your Web server is not recognized by Setup, you must publish the Publish directory to the Web. Refer to the Web server documentation for information on how to publish the directory.
7. Restart the Web server.
8. Now that your installation is complete, see Part 3, "Configuring Host On-Demand" on page 71.

At the end of installation, the Host On-Demand Service Manager is started automatically.

Installing Host On-Demand in silent mode

A silent installation installs Host On-Demand without displaying any windows or asking for input. All of the input required during an installation is obtained from a text file called a response file. A response file is created by recording an installation. The response file is included in the instmgr directory as install.script. The defaults are English, no WebServer configuration, no WebSphere configuration, and a port value of 8999. If these values are not correct and there is not a GUI–capable console available to record a new response file, the install.script file may be copied to a writeable directory and manually edited based on the comments included in the install.script file.

A local client cannot be installed silently.

When you install in silent mode, there is no indication that installation is in progress or that it is complete.

To record a response file:

```
setup.exe -r -f1d:\temp\server1.iss
```

To install in silent mode:

```
setup.exe -s -f1d:\temp\server1.iss -f2d:\temp\server1.log
```

Options supported in silent mode:

-r	Records a response file
-s	Runs a response file and installs Host On-Demand
-f1[path\response_file_name].iss	Defines the response file, in both record and run modes. The path and filename must be 43 characters or fewer. There must not be a space between parameter and value. The filename extension **must** be `iss` .
-f2[path\log_file_name]	Defines the log file and can be used in run mode to create a file that contains a history of an installation. The path and filename must be 43 characters or fewer. There must not be a space between parameter and value.

The target system's configuration **must** be the same as that of the source system (the system on which the response file was created). For example, if the source system has a previous installation of Host On-Demand 6.0, the target system must have the same. If the source system installed Host On-Demand on the D drive, the target system must also have a D drive. The source and target systems must have the same number of Web servers, although they do not need to be the same types.

Format of the silent mode installation log file: If an installation is not successful, the log file might indicate the reason. The format of a log file is as follows:

```
[InstallShield Silent]
Version=v7.00.000
File=Log File
[Application]
Name=\Host On-Demand Server
Version=7.00.000
Company=IBM
[ResponseResult]
ResultCode=0
```

Result code values: The ResultCode indicates whether or not the installation was successful. Possible values are:

-0	Successful
-1	General error
-2	Mode not valid
-3	Required data not found in the response file
-4	Not enough memory available
-5	File does not exist
-6	Cannot write to the response file
-7	Cannot write to the log file
-8	Path to the response file is not valid
-9	Not a valid list type (string or number)
-10	Data type is not valid
-11	Unknown error during setup
-12	Dialogs are out of order. Since the dialog order depends on what other related products were already installed on the workstation, the target system must have the same products.
-51	Cannot create the specified folder
-52	Cannot access the specified file or folder
-53	Selected option is not valid

Common silent installation problems:

- The `setup.iss` file is not in the directory specified by the -f1 option.
- You changed the name or location of the `setup.iss` file and did not specify the new name or location when you ran the `setup.exe` command to install the product.
- There is not enough space on specified target drive to install the product.
- You are installing or uninstalling Host On-Demand and you are not logged on to the target machine with Administrator authority.
- There is an error in the syntax of the `setup.exe` command.

After installing Host On-Demand on a machine running Microsoft Personal Web Server, the virtual directory for Host On-Demand does not show up in the list of virtual directories in the Personal Web Manager GUI. Therefore, after the installation is complete, do not restart the Web server using the Start/Stop button in the Personal Web Manager GUI. Instead, restart the Web server using the Services GUI in Windows. You can also manually add the directory to the list of virtual directories in the Personal Web Manager GUI.

Installing on AIX

You can automatically install Host On-Demand through a graphical interface, or through an ASCII control file in silent mode.

The automatic installation verifies the presence and version of required products before installation occurs. If a prerequisite is missing the action taken by the Install Manager will depend on the policy setting in the control file.

Installing Host On-Demand using the graphical interface

To install the Host On-Demand server on a AIX workstation using the graphical interface, follow the steps below.

1. Insert the CD and mount the CD-ROM drive.
2. Start the installation program by changing to the root directory of the CD, type `setupaix.sh` and press Enter. You may need to type`./setupaix.sh` if the current directory (.) is not set in your `PATH` variable. The AIX install program window appears.
3. Optionally, click on View Documentation to see the product documentation (including these installation instructions).

Make sure you have configured Netscape such that it can be run by the installation program. Specifically, before running setupaix.sh, ensure that the Netscape executable is in your PATH (e.g. /usr/local/netscape), and that MOZILLA_HOME is set to the appropriate directory (e.g. /usr/local/netscape).

4. Click Install Product.
5. Follow the directions in the installation windows.
   - The default server directory, determined by the installation program, is `/usr/opt/hostondemand` . The server directory contains files used only by the server and must not be available to client workstations.
   - The default publish directory, determined by the installation program, is `/usr/opt/hostondemand/HOD` . The publish directory contains files that must be available to client users who access the server through a browser.
   - The default Service Manager port is 8999, and it is usually a safe port to select. Check your server documentation to see if this port is being used. If it is in use, you can change the port later. For more information about changing the Service Manager port, see Changing the Service Manager’s configuration port in the online help.
   - If the installation program detects IBM WebSphere Application Server, Lotus Domino Go Web Server, or IBM Domino Go Web Server installed, you are asked if you want to use the configuration servlet to connect to the configuration server for client configuration information. If you are running Host On-Demand through a firewall, this eliminates the need to open an extra port for the configuration server. Answering Yes automatically configures the clients to access the configuration server through the configuration servlet. Answering No configures the clients to access the

configuration server directly on port 8999. See “Installing the configuration servlet” on page 59 for more information.

6. Click finish to end the installation.
7. If a message tells you that your Web server was not recognized or was not configured, configure it. If you install a Web server later or your Web server was not recognized by the Install Manager, you must publish the Host On-Demand Publish directory to the Web. Refer to the Web server documentation for information on how to publish the directory.
8. Restart the Web server.
9. Now that your installation is complete, see Part 3, “Configuring Host On-Demand” on page 71.

Installing Host On-Demand in silent mode

A silent installation installs Host On-Demand without displaying any windows or asking for input. All of the input required during an installation is obtained from a text file called a response file. A response file is created by recording an installation.

When you install in silent mode, there is no indication that installation is in progress or that it is complete.

Options supported in silent mode

Command Line Option	Description
-r	Records a response file.
-p	Runs a response file to install Host On-Demand.
/path/response_file_name	Defines the name for the response file. The default is install.script, and a sample install.script file is provided in the \instmgr directory on the Host On-Demand CD. Any file name can be used if properly specified on the command line used to execute the installation process.

Below are sample command lines that will install Host On-Demand on an AIX workstation in silent mode. The silent mode installation installs Host On-Demand in the `/usr/opt` directory, creates `hostondemand` as the server directory and `HOD` as the publish directory. The examples assume that you mounted the CD-ROM drive as `/cdrom` .

The following commands must be on one line. Before issuing any of the following commands change into the instmgr directory, for example. `cd /cdrom/instmgr`.

To install in silent mode using the `install.script` from the CD and record a log file called HodInstall.log:

```
/cdrom/instmgr/instaix.sh -p /cdrom/instmgr/install.script > /tmp/HodInstall.log
```

To record a response file:

```
/cdrom/instmgr/instaix.sh -r /tmp/install.script
```

To playback the response:

```
/cdrom/instmgr/instaix.sh -p /tmp/install.script
```

The target system's configuration **must** be the same as that of the source system (the system on which the response file was created). For example, if the source system has a previous installation of Host On-Demand Version 6, the target system must have the same. If the source system installed Host On-Demand to a /usr/opt/hostondemand directory, the target system must also have a /usr/opt/hostondemand directory. The source and target systems must have the same number of Web servers, though they do not need to be the same type.

Installing on the Solaris, HP-UX, and Linux platforms

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

To install the Host On-Demand server on Solaris, HP-UX and Linux workstations, follow the steps below. These examples assume that you are installing Host On-Demand in the /usr/local directory and that hostondemand is the server directory and HOD is the publish directory. Adjust the statements to match your environment.

1. Insert the CD and mount it.
2. Change to the /usr/local directory and create a server directory, for example, hostondemand . The server directory contains files that are used only by the server and must not be available to client workstations.

   ```
   cd /usr/local
   mkdir hostondemand
   ```
3. Change to the server directory, and untar the files from hod70srv.tar to the server directory. Tar files are located in the /cdrom/tar directory.

   ```
   cd hostondemand
   tar -xf /cdrom/tar/hod70srv.tar
   ```
4. Create the HOD directory, which is the Publish directory.

   ```
   mkdir HOD
   ```
5. Change to the HOD directory, and untar hod70www.tar into the HOD directory.

   ```
   cd HOD
   tar -xf /cdrom/tar/hod70www.tar
   ```

   English language support is installed by default. If you want additional language support, untar the appropriate language file from the /cdrom/tar directory. For example, to install Spanish language support, do the following:

   ```
   cd HOD
   tar -xf /cdrom/tar/hod_es.tar
   ```
6. Make the publish directory, /usr/local/hostondemand/HOD available to clients on the network. Refer to your Web server documentation for information about how to do that.
7. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application:
   a. Change directory to the /usr/local/hostondemand/lib subdirectory.
   b. Copy NCServiceManager-UNIX from the /usr/local/hostondemand/lib/samples/CommandFiles directory.

Make sure the NCServiceManager-UNIX file has execute permission.

c. Edit NCServiceManager-UNIX to reflect the directory paths that are correct for your workstation.

d. Run NCServiceManager-UNIX . The Service Manager does not display a message indicating that it has started. To arrange for this script to be run at boot time, refer to the documentation supplied with your operating system to add a boot service. Also, disregard the following message: *Native library failed to load, indicating this Redirector does not support SSL.* The failure to load this library simply indicates that the server does not support SSL sessions.

For Host On-Demand to function, the Service Manager must be running. If you reboot the server, you must also restart the Service Manager.

8. Restart the Web server.
9. Now that your installation is complete, see Part 3, “Configuring Host On-Demand” on page 71.

Installing on OS/2

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

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

1. Insert the CD.
2. Create a server directory, for example, hostondemand . The server directory contains files that are used only by the server and must not be available to client workstations.
3. Change to the server directory.
4. Run the following command to extract the files:

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

   where:
   - *unzip* is your unpacking program (such as UNZIP.EXE). It must support long file names
   - *[cd_rom]* is the CD-ROM drive letter
   - *zip* is the directory on the CD
5. Create the publish directory; for example, HOD. The publish directory contains files that must be available to client users who access the server through a browser.
6. Change to the publish directory.
7. Run the following command to extract the files:

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

   ```
   ifconfig lo 127.0.0.1
   ```

10. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application:
    a. At the command prompt, change directory to `\hostondemand\lib` .
    b. Copy `NCServiceManager-OS2.cmd` from the `\hostondemand\lib\samples\CommandFiles` directory.
    c. Edit `NCServiceManager-OS2.cmd` to reflect the directory paths appropriate for your workstation.
    d. Run `NCServiceManager-OS2.cmd`. The Service Manager does not display a message indicating that it has started. Also, disregard the following message: *Native library failed to load, indicating this Redirector does not support SSL.* The failure to load this library simply indicates that the server does not support SSL sessions.

For Host On-Demand to function, the Service Manager must be running. If you reboot the server, you must also restart the Service Manager. You might want to add the `NCServiceManager-OS2.cmd` command to your `startup.cmd` file so that the Service Manager starts automatically when the workstation boots. If you do, remember to specify the path to change directory to the `\hostondemand\lib` subdirectory before the command runs.

11. Restart the Web server.
12. Now that your installation is complete, see Part 3, “Configuring Host On-Demand” on page 71.

Installing on Novell NetWare

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

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

1. Stop the Service Manager with the `java -exit` command.
2. From a client workstation, map a drive to the `SYS:` volume of the Novell server.
3. Insert the CD.
4. Create a server directory, for example, `hostondemand`. The server directory contains files that are only used by the server and must not be available to client workstations.
5. Change to the server directory.
6. From the drive mapped to the `SYS:` volume, run the following command to extract the files:

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

   where:
   - *unzip* is your unpacking program (such as `WinZip`). It must support long file names.
   - *[cd_rom]* is the CD-ROM drive letter.
   - *zip* is the directory on the CD.

7. Create a publish directory named `HOD` and change to that directory. The `HOD` directory contains files that must be available to client users who access the Host On-Demand server through a browser.
8. Run the following command to extract the files:

   ```
   unzip [cd_rom]:\zip\hod70www.zip
   ```
9. From the server console, run the command `load java` to start the Java NLM.
10. Start the Host On-Demand Service Manager, which provides support services for Host On-Demand and runs as a Java application, by following these steps from a client system mapped to the `SYS` volume of the server:
    a. Copy `NCServiceManager-Novell.ncf` from the `\hostondemand\lib\samples\CommandFiles` directory to the `\system` directory on the Novell server. To run the command from the server console, you might have to change the file name to the eight-dot-three format.
    b. Edit `NCServiceManager-Novell.ncf` (or the eight-dot-three format of the file) to reflect the directory paths that are correct for your workstation.
    c. From the server, run `NCServiceManager-Novell.ncf` (or the eight-dot-three format of the file). The Service Manager does not display a message indicating that it has started.

For Host On-Demand to function, the Service Manager must be running. If you reboot the server, you must also restart the Service Manager.

11. Now that your installation is complete, see Part 3, “Configuring Host On-Demand” on page 71.

Installing the configuration servlet

During the Host On-Demand installation, you can choose to have the configuration servlet installed and configured on the Windows NT, Windows 2000, and AIX platforms for recognized Web application servers. Recognized Web application servers include:

- IBM WebSphere Application Server Version 3.5 and 4.0
- Lotus Domino Go Web Server
- IBM Domino Go Web Server

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

Installing the configuration servlet on the Windows and AIX platforms

The following instructions assume a Web server is already installed. To manually install the configuration servlet:

1. Install Host On-Demand, without running the configuration servlet installation, to a directory such as `d:\hostondemand` or `/usr/opt/hostondemand`.
2. Add `cfgsrvlt.jar` from the Host On-Demand installation’s `lib` directory to the servlet engine’s classpath; for example `d:\hostondemand\lib\cfgsrvlt.jar` or `/usr/opt/hostondemand/lib/cfgsrvlt.jar`. Refer to your Web server or servlet engine documentation for information about how to do this. You can get a copy

of `cfgsrvlt.jar` from the `/servlet` directory of the Host On-Demand CD or from the *`install_dir`*`/hostondemand/lib` directory on your server.

3. Add a servlet definition named `hodconfig` with a class name of `com.ibm.eNetwork.HODUtil.services.remote.HODCfgServlet`. Refer to your Web server or servlet engine documentation for information about how to add a servlet definition.
4. Configure the configuration servlet. If necessary, set the `ConfigServer` and `ConfigServerPort` parameters to the host name and port number of the Host On-Demand Service Manager. Refer to your Web server or servlet engine documentation for information about how to pass parameters to a servlet.

   The port used by the clients, configuration servlet, and the Service Manager can be customized. For instructions on how to customize the port, see the topics Configuring the configuration servlet and Changing the Service Manager port in the online help.

   Host On-Demand clients use the default port of 8999 to communicate with the Service Manager for configuration information. If any of your clients are outside the firewall, the firewall administrator must open this port internally and externally. Optionally, you can customize the clients to access the configuration servlet through a firewall over either HTTP or HTTPS. The configuration servlet then communicates with the Service Manager on port 8999. If both the configuration servlet and the Service Manager are inside the firewall, port 8999 does not need to be opened for Host On-Demand.
5. Publish the `hodconfig` servlet using an alias. Refer to your Web server or servlet engine documentation for information on about how to make the configuration servlet known to the Web server. In general, you are associating the fully qualified name of the servlet with an alias.
6. Stop and restart the Web server and the servlet engine, or refer to your Web server or servlet engine documentation for information about saving the changes.

Once the configuration servlet is installed, you must configure your clients to use the configuration servlet instead of directly accessing the Service Manager. You can use the Deployment Wizard to build customized HTML client pages. The wizard sets the applet parameters in the HTML based on your input, so you don’t have to learn the syntax and valid parameter values. We recommend that you use the Deployment Wizard to set the ConfigServerURL parameter in the client HTML to the name you assigned to the servlet through the servlet engine in the publish step above. For example, if you set the name of the servlet to be `/servlet/hodconfig`, set the Configuration Server URL to `/servlet/hodconfig/hod`.

The servlet alias and the value for the `ConfigServerURL` parameter are different.

If you find you need to manually modify the HTML, use the <*param tag*> inside the <*applet*> tag to set the ConfigServerURL. For example, to set the `ConfigServerURL` to `/servlet/hodconfig/hod` set `<param name=ConfigServerURL value=/servlet/hodconfig/hod>` in the <*applet*> tag in the HTML client.

For more information regarding configuration servlet parameters, configuration and examples, see Configuring the configuration servlet in the online help.

Installing the configuration servlet on the iSeries platform

On the iSeries platform, you must manually run a separate utility in order to install and configure the configuration servlet. This utility is provided by Host On-Demand and supports WebSphere Application Server Version 3.5 and 4.0.

To install and configure the configuration servlet on iSeries, do the following:

1. Start a shell by entering the following at the command prompt:
   ```
   qsh
   ```
2. Change directories to the Host On-Demand servlet directory:
   ```
   cd /qibm/proddata/hostondemand/lib/samples/hodservlet
   ```
3. Enter the following command to run the configuration utility:
   ```
   cfghodservlet-os400.sh
   ```

   The installation is complete when the $ symbol is shown.
4. Press the F3 key to exit the qsh program.
5. Edit the config.properties file by entering the following at the command prompt:
   ```
    edtf '/qibm/proddata/hostondemand/hod/config.properties'
   ```
6. Add the following line:
   ```
   ConfigServletURL=http://my400/HOD/HODConfig/hod
   ```

   where *my400* is the name of the iSeries system. Be aware that this URL is case sensitive.
7. Press the Enter key, then press the F3 key to update the config.properties file.
8. Stop the Host On-Demand Service Manager by entering the following command at the command prompt:
   ```
   ENDHODSVM
   ```
9. Restart the Host On-Demand Service Manager by entering the following command at the command prompt:
   ```
   STRTHODSVM
   ```
10. Verify that the servlet is working. In a Web browser, enter the following URL:
    ```
    http://my400/HOD/HODConfig/info
    ```

    where *my400* is the name of the iSeries system. Be aware that this URL is case sensitive.

Installing the Deployment Wizard

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

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

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

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

Installing the Deployment Wizard from the Windows CD

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

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

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

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

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

1. From your Windows machine, start your browser and point to the HODMain_*xx*.html file on your Host On-Demand server, where *xx* is your two letter language suffix.
2. Click on the Deployment Wizard link. This will download the Deployment Wizard installation image to your Windows machine.
3. Run the Deployment Wizard installation from your Windows machine.
4. Once installation is complete, you can launch the Deployment Wizard from the Start > Programs desktop menu.

Chapter 8. Upgrading from earlier versions of Host On-Demand

Upgrading the Host On-Demand server

Backing up files and directories

You can upgrade the Host On-Demand server so that the upgrade is transparent to the clients. After the upgrade, the clients have their same sessions defined and all their customizations, for example, macros and keyboard remaps, continue to work as before. On platforms where an uninstall program for Host On-Demand is not provided, the administrator must back up some files and directories before upgrading, and then restore them after the upgrade.

The method for backing up files might vary depending on what server platform you use.

If you need to make changes to the NSMprop file (for example, to change the default port), or need to migrate NSMprop from a previous version of Host On-Demand, put this file in the /private directory.

Setting up a separate user publish directory

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

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

1. Specify the codebase (the URL of your Host On-Demand publish directory) as follows:
   a. Using the Deployment Wizard, on the Additional Options page, click the Advanced Options button.
   b. Select the Other tab.
   c. Enter the codebase. You can enter a fully qualified URL including the hostname (for example, http://your_HOD_server/hod_publish_dir_alias/) or a relative path (for example, /hod_publish_dir_alias/).
2. Select Output Zip to save the files generated from the Deployment Wizard in a Zip file.
3. Click Create HTML.
4. If you are not running the Deployment Wizard on your Host On-Demand server, FTP the output Zip file to your server platform.
5. Create a separate user publish directory, /user_publish_dir/.
6. Use the DWunzip tool to install the Deployment Wizard generated files into the /user_publish_dir/ directory. You must edit the Dwunzip command file

on your server to specify the correct MY_PUBLISHED_DIRECTORY value. See the online help topic Using Dwunzip for more information on how to use this tool.

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

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

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

8. If changes are required in the Host On-Demand config.properties file (for example, to change the default port or enable the Host On-Demand configuration servlet), do the following:
   a. Update the config.properties file. If your server platform does not support the ASCII character set, update this file on a machine that does support ASCII.
   b. If the config.properties file was updated on a different platform than your server, FTP the file to your server platform in binary format.
   c. Place the file in the user publish directory, /user_publish_dir/.
   d. Add the following pass rule (also known as an alias on some platforms) in the Web server configuration file /etc/httpd.conf:

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

On the zSeries platform, append the ascii extension, /user_publish_dir/config.properties.ascii.

9. If you are using SSL and need to change the CustomizedCAs.class file, do the following:
   a. Place the updated file in the user publish directory /user_publish_dir/CustomizedCAs.class.
   b. Add the following pass rule (also known as an alias on some platforms) in the Web server configuration file /etc/httpd.conf:

      ```
      /hod_publish_dir_alias/CustomizedCAs.class
      /user_publish_dir/CustomizedCAs.class
      ```

10. Restart the Web server.
11. From a Web browser, specify the URL: http://your_HOD_server/user_alias/your_html.html.

Migrating on server platforms with an uninstall program

On server platforms that have an uninstall program, for example, Windows and AIX, the uninstall program assists in the upgrade process. The uninstall program does not uninstall any files that the installation program did not install initially, for example, CustomizedCAs.class or customized HTML files. Also, there are no changes to the private directory during the uninstall of the previous release. Any customized files that you added for the previous release of Host On-Demand remain unchanged when you install Host On-Demand 7. Run the uninstall program to remove the old version and then install Host On-Demand 7.

Migrating on server operating systems without an uninstall program

On server platforms without an uninstall program, you should delete the Host On-Demand 6 installation directory. Before you delete the installation directory, copy the private directory, any files added to the publish directory, such as CustomizedCAs.class or customized HTML files, and the HODData directory to a temporary location. After you install Host On-Demand 7, move these files and directories back to their original location.

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

If you install Host On-Demand in a test environment before deploying to your production environment, complete the following steps to migrate Host On-Demand from one server to another (or from one HFS to a different HFS in an OS/390 or z/OS environment). First, install Host On-Demand on the new server. Then copy the private directory, any files added to the publish directory, such as CustomizedCAs.class or customized HTML files, and the HODData directory from the test environment to the new server environment.

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

Upgrading the Host On-Demand client

Download client users load the new Host On-Demand 7 client code the first time they point their browsers to the Download client HTML file after the Host On-Demand server has been updated to HOD 7. They will be able to use the new features of Host On-Demand 7 right away.

The cached client code detects that there is a newer version available on the server. Depending on how you set the cached client upgrade controls, users could be delayed in upgrading to the newer version. They will not be able to take advantage of the new features until their client code gets upgraded, but they can continue to use the older cached client code until then.

Upgrading Host On-Demand Version 4.x cached clients to Host On-Demand 7

If you upgrade your Host On-Demand server from Version 4.x to Version 7, your clients will no longer be able to communicate with the server without upgrading.

If you need to manage network demand while upgrading cached clients, you can gradually move all of your Host On-Demand Version 4.x cached clients to Host On-Demand 7 by setting up two servers. One would be a Host On-Demand Version 4.x server and the other would be a Host On-Demand 7 server. Configure all clients to access the Host On-Demand 7 server, and then add the HTML parameter HODServer to HODCached.html, or any of your customized cached client HTML files that are on the Host On-Demand 7 server. There are two sets of applet parameters defined in the HTML. Add the HODServer parameter to the set defined by the array cHod_AppletParams. You can do all of this using the Deployment Wizard on the Additional Parameters window; however, if you want to manually modify the HTML, the format for the parameter is:

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

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

The *HODServer* parameter works with the UpgradePercent and UpgradeURL parameters to manage client upgrades. If the cached client won't be upgraded on this connection attempt, it is redirected automatically to the Host On-Demand Version 4.x server specified in the *HODServer* HTML parameter. If a cached client will be upgraded, the Host On-Demand Version 4.x cached client is removed and the Host On-Demand 7 cached client is installed. Once the client is upgraded to Host On-Demand 7, the HTML parameter is ignored and the client is no longer redirected to the Host On-Demand Version 4.x server. After you have gradually upgraded all your cached clients, you no longer need the Host On-Demand Version 4.x server.

Be aware of the following when you are upgrading cached clients from Version 4.x to Version 7:

- Cached clients are upgraded in the foreground. The upgrade in background option is ignored.
- If you have customized Host On-Demand Version 4.x `HODCached.html` and have called it something different, like `OurHTML.html`, do the following:
  1. Copy the Host On-Demand 7 version of `HODCached.html` to the file `OurHTML.html`;
  2. Add the `HODServer` parameter to `OurHTML.html`. The `HODServer` parameter should specify `http://yourhostname/alias/OurHTML.html` as the Host On-Demand Version 4.x server.
- You can copy the new `HODCached.html`, that includes the `HODServer` parameter, to `AutoHODCached.html` and `AutoHODLaunch.html`, in case these pages are bookmarked by the clients. The `HODServer` parameter in `AutoHODCached.html` should specify the `AutoHODCached.html` page on the Host On-Demand Version 4.x server. The `HODServer` parameter in `AutoHODLaunch.html` should specify the `AutoHODLaunch.html` page on the Host On-Demand Version 4.x server
- If you are using language specific HTML files (such as `HODCached_es.html`, `AutoHODCached_es.html`, `AutoHODLaunch_es.html`, etc.) you can also add the `HODServer` to these pages.

Upgrading custom HTML files

Java 1

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

Java 2

If your users have Java 2 browsers, we strongly encourage you to regenerate the HTML files with the Host On-Demand 7 Deployment Wizard to receive the improved support for Java 2 environments. Additionally, if you want to take advantage of the new features built in to the Host On-Demand 7 Deployment

Wizard, such as the customized template, separate codebase, or upgrade based on time of day, you should regenerate your custom HTML files.

Upgrading from Java 1 to Java 2 on the client

The IBM Java 2 plug-in for Windows is installed on the server as part of the Host On-Demand server installation. To install the plug-in on the client, load HODMain_*xx*.html in your browser, where *xx* is your two letter language suffix, and click on Java 2 Runtime Environment for Windows. When Host On-Demand detects that Windows clients require a Java 2 plug-in, they will be directed to this Web page, where they can download and install the plug-in. Clients on other platforms should refer to the Sun Microsystems Web site, http://www.javasoft.com, for details on installing a Java 2 plug-in.

Upgrading to Host On-Demand 7 and Java 2 at the same time will require an additional download of the Host On-Demand cached client. To avoid this, install Java 2 before upgrading to Host On-Demand 7.

Additional information on planning for Java 2 implementation on the client may be found in Chapter 4, “Planning for Java 2 on the client” on page 23.

Chapter 9. Uninstalling the Host On-Demand server

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

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

iSeries
You will need `*JOBCTL`, `*SPLCTL`, `*SERVICE` and `*ALLOBJ` authority to use this command. Logon to the iSeries with a security officer user profile, such as `QSECOFR` .

1. Shutdown the Service Manager by typing `ENDHODSVM` at the command line.
2. Delete the licensed Host On-Demand product by typing `DLTLICPGM LICPGM(5733A59)` at the command line.
3. Remove any directories containing user data manually after the program has completed. You will also need to remove the `QUSRSYS/QHODCFGD *DTAARA` object.

Windows NT, Windows 2000, or Windows XP
Use Add/Remove Programs from the Windows control panel.

Notes:

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

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

AIX, Solaris, Linux, HP-UX
Stop the Host On-Demand Service Manager. Get the process ID, kill the process, then delete the Host On-Demand directories (except `./private`).

OS/2
Stop the Host On-Demand Service Manager by pressing `Ctrl+C` in the OS/2 window in which you started it, close the window, then delete the Host On-Demand directories (except `\private`).

Novell NetWare
From the console, enter `java -exit` to stop the Java NLM, then delete the Host On-Demand directories (except `\private`).

Part 3. Configuring Host On-Demand

Chapter 10. Configuring Host On-Demand emulator clients

After installing Host On-Demand, you will need to create HTML files and configure Host On-Demand sessions for your users.

Creating Host On-Demand HTML files

The best way to create and set up your HTML files for Host On-Demand is to use the Deployment Wizard. The Deployment Wizard allows you to easily create custom HTML files that contain all of the Host On-Demand features tailored for your environment. The following is a list of some of the many features that can be configured using the Deployment Wizard:

- **Configuration models**. Configuration models define the high-level approach you wish to follow with regard to where you define your sessions and where any user preferences are kept. For more information about configuration models, refer to Chapter 3, “Planning for deployment” on page 19.
- **Preloads**. Host On-Demand runs as an applet and must download code to the users’ machines. By default, the Host On-Demand client downloads all of the components, but you may reduce the download size by removing those components that are not needed.
- **Download or cached client**. Download clients download the necessary applet files each time users access the HTML files; cached clients retain the code the first time users access the HTML page, and store it on the users’ machines.
- **Web page appearance (custom HTML templates)**. You can easily set up a template that the Deployment Wizard will use to generate your HTML files. This feature makes it easy to add your own background, banners, etc.
- **Client Java level**. Clients running Java 2-enabled browsers will need somewhat different HTML files than those running Java 1-enabled browsers. In the Deployment Wizard, you can select Java 1, Java 2, or Auto-detect.
- **Cached client upgrade options**. When running the cached client, the code must be upgraded when newer versions of the client are available. There are a number of Deployment Wizard options that allow you to control when the upgrades are done.
- **Location of the Host On-Demand install (codebase)**. Usually, Deployment Wizard files are placed in the Host On-Demand server’s publish directory. However, sometimes it may be useful to put these files in a location that is independent of the Host On-Demand server so that they can be granted different security controls or make Host On-Demand server upgrades easier, for example.
- **Locale options**. The Host On-Demand applet will automatically display client desktop and session frame messages in the language identified by the locale on users’ machines. However, using the Advanced Options tab on the Deployment Wizard, you can specify a particular locale to use if you wish to ignore the setting on each user’s machine.
- **Windows Domain logon**. If your users are logged on to a Windows domain, this option automatically logs users on to Host On-Demand using their Windows user name. This option is available only when using the configuration server-based model in the Deployment Wizard.
- **Session Manager APIs**. The Host On-Demand Session Manager provides JavaScript APIs for managing host sessions and text-based interactions with host

sessions. These APIs are intended to provide support for embedding host sessions into a Web page using JavaScript and can be enabled with the Deployment Wizard.

In addition to creating custom HTML files with the Deployment Wizard, another way to access Host On-Demand is to use one of a number of predefined HTML files that are installed with your server. These predefined HTML files are general-purpose HTML files, and they all support the configuration server-based model. Note that Database On-Demand is only available using these predefined HTML files.

Configuring Host On-Demand sessions

In addition to setting up your HTML files, you will need to define sessions for your users. If you are using the HTML-based model, then you configure your sessions in the Deployment Wizard at the same time that you create the HTML files. Otherwise, if you are using the configuration server-based model or the combined model, or using one of the predefined clients, you will need to create groups, users, and sessions in the configuration server using one of the administration clients.

There is a full range of options available to you when you are configuring your sessions, regardless of whether you need to use the Deployment Wizard or one of the administration clients:

- **Session properties**. All of the session properties can be configured, including connection information, security, etc. Each of the fields may be locked to prevent users from updating them.
- **Runtime options**. When configuring a session, you can launch the session and configure features such as session size and placement, colors, toolbar customization, and macros.
- **Disabling user functions**. You can disable almost any of the functions that users normally receive as part of their Host On-Demand session, such as bookmarking, creating or running macros, etc.

Using the Deployment Wizard

The Deployment Wizard runs on a Windows platform. To start the Deployment Wizard, select one of the following ways:

- If you automatically installed the Deployment Wizard as part of the Windows Host On-Demand server, go to Start > Programs > IBM Host On-Demand > Deployment Wizard.
- If you installed the Deployment Wizard from the Windows CD separately, go to Start > Programs > IBM Deployment Wizard > Host On-Demand Deployment Wizard.

For more information about installing the Deployment Wizard, see “Installing the Deployment Wizard” on page 61.

The Deployment Wizard guides you through configuration choices and provides comprehensive help for the features. When you have finished selecting features, the Deployment Wizard creates the HTML and supporting files for you. These files need to be placed on the Host On-Demand server in a directory known to your Web Server; usually, this directory is your Host On-Demand server’s publish directory.

Distributing the Deployment Wizard output to your Host On-Demand server

If your Host On-Demand server is on a Windows or AS/400 platform, you may be able to write your Deployment Wizard HTML and configuration files directly to your Host On-Demand server's publish directory. On the final screen of the Deployment Wizard, you can select where to write the generated files. You may select any local or network drive accessible by the machine where your Deployment Wizard is running. In this case, you would direct the Deployment Wizard output to a publish directory on the Host On-Demand server and specify an output format of *HTML*. Assuming that you have already defined your sessions, the HTML page is then ready to be accessed by your users.

Otherwise, if your Deployment Wizard cannot directly write to your Host On-Demand server, then you should select to have the Deployment Wizard generate a zip file for the output format. The Deployment Wizard will then produce a single zip file containing all of the HTML and supporting files. You will need to move the zip file to the Host On-Demand server and use DWunzip to explode the zip file into the desired publish directory. Assuming that you have already defined your sessions, the HTML page is then ready to be accessed by your users.

Chapter 11. Using Host On-Demand administration and new user clients

Host On-Demand supplies several predefined clients for administering Host On-Demand and creating new user accounts. Before accessing an emulator client or a Database On-Demand client that uses the configuration server-based or combined deployment models, you must add users and configure sessions for them with one of the administration or full administration clients.

Loading administration and new user clients

To load an administration or new user client, do one of the following:

- Specify the full URL of the HTML file in your browser:

  ```
  http://server_name/hod_alias/client_name.html
  ```

  where *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_name* is the HTML file name of the administration or new user client. For example, you can download the cached version of the administration client from the Web server by specifying a URL such as the following:

  ```
  http://host.yourcompany.com/hod/HODAdminCached.html
  ```

- Load the HODMain_*xx*.html file, where *xx* is your two-letter language suffix, into your browser to view links to all the available administration and new user clients, plus other predefined clients. HODMain_xx.html is located in the publish directory.

Administration clients

Administration clients enable you to perform the following tasks for data stored on the configuration server:

- Manage users, groups, and sessions
- Configure, manage and trace the Redirector service
- Configure Database On-Demand
- Enable security
- View trace and message logs
- Disable functions to end users

Administration clients run on all Host On-Demand client platforms. If you are creating HTML files in the Deployment Wizard using either the configuration server-based or combined models, you must configure sessions on the configuration server using an administration client. Refer to Basic Configuration Steps in the online help for more detailed information about configuring the Host On-Demand configuration server.

Host On-Demand supplies the following predefined administration and full administration clients:

There will be a delay using predefined HTML files if you use Internet Explorer only with Java 1. To avoid this delay, you can edit the HTML and change the hod_JavaType JavaScript variable from a value of 'detect' to 'java1'.

Administration client (HODAdmin.html)

Loads the download version of the administration client.

Administration client cached (HODAdminCached.html)

Loads the cached version of the Administration client. The advantage of using this client is that it can be cached along with the cached client in the browser.

To bookmark the cached Administration client, you must manually create the bookmark. It must point to HODAdminCached.html, so that Host On-Demand can compare the cached version to the server version. This allows Host On-Demand to recognize and notify you that a newer version of the cached Administration client is available at the server.

Administration client cached with problem determination (HODAdminCachedDebug.html)[1]

Loads the Administration client in a cached environment with problem determination (session logging and tracing) enabled.

Full Administration client (HODAdminFull.html)[2]

Loads the download version of the full Administration client. The full administration client gives the administrator the additional ability of starting sessions to configure runtime properties. However, the download size of the full administration client is larger than the download size of administration client.

Full Administration client cached (HODAdminCachedFull.html)[2]

Loads the cached version of the full Administration client. Like the cached version of the regular Administration client, this client can be cached along with the cached client in the browser.

Full administration client cached with problem determination (HODAdminCachedDebugFull.html)[1, 2]

Loads the cached version of the full Administration client with problem determination (session logging and tracing) enabled.

Notes:

1. Use the problem determination clients only if you are working with Support to resolve a problem with your Host On-Demand installation.
2. The full Administration client is the Administration client with Start Session enabled.

Directory Utility

Directory Utility is a command-line Java application the administrator can use to manage user, group or session configuration information. This information is stored either in the Host On-Demand default data store, or in an LDAP directory. This utility is only useful in the environment where the Configuration Server-based model is in use. Directory Utility allows you to add, delete, or update large numbers of users, groups, or sessions in a batch mode environment instead of using the Administration client. Directory Utility reads an XML ASCII file that contains the following actions to be performed on users, groups, or sessions defined to the Configuration Server:

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

For more information, see Using the Directory Utility in the online help.

New user clients

If the administrator has enabled **Allow users to create accounts** in the **Users/Groups** window, users can use the predefined new user clients to create new accounts. See the New User client topic in the online help for more information about this client.

There will be a delay using predefined HTML files if you use Internet Explorer only with Java 1. To avoid this delay, you can edit the HTML and change the hod_JavaType JavaScript variable from a value of ’detect’ to ’java1’.

The following new user clients are supplied with Host On-Demand:

New user client (NewUser.html)
Loads the download version of the New user client.

New user client cached (NewUserCached.html)
Loads the New User client in a cached environment.

New user client with problem determination (NewUserCachedDebug.html)[1]
Loads the New User client in a cached environment with problem determination (session logging and tracing).

Notes:

1. Use the problem determination clients only if you are working with Support to resolve a problem with your Host On-Demand installation.

Chapter 12. Using Host On-Demand emulator clients

This chapter discusses issues that you need to be aware of when configuring and using Host On-Demand terminal emulator clients.

- “Loading emulator clients” describes how to access Host On-Demand clients.
- “Cached clients” on page 82 discusses how to use cached clients, including installing and removing them, deploying them over the Internet, using them with Windows restricted users, upgrading them, and troubleshooting problems with them.
- “Download clients” on page 86 discusses how to use download clients, including installing them and loading them after downloading a cached client.
- “Predefined emulator clients” on page 88 describes the predefined emulator clients supplied with Host On-Demand.
- “Selecting download client vs. cached client” on page 87 discusses how to decide which client is best for your needs.
- “Function On-Demand client (HODThin.html)” on page 87 describes the Function On-demand client.
- “Reducing client download size” on page 88 discusses strategies for reducing the download size of clients.

Loading emulator clients

Host On-Demand emulator clients are launched by HTML files that you load into a Web browser. In general, it is recommended that you customize your own HTML files to launch sessions that you have configured. You can use the Deployment Wizard to create customized HTML files. See the Deployment Wizard topic in the online help for more information. Alternatively, you can load one of the predefined emulator clients described in “Predefined emulator clients” on page 88.

If your emulator client is deployed with the configuration server-based or combined deployment model, you must add users and configure sessions with the administration client before you can use the emulator client.

Regardless of which type of HTML file you plan to use, do one of the following to load it:

- Specify the full URL of the HTML file in your browser:.

  ```
  http://server_name/hod_alias/client_name.html
  ```

  where *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_name* is the HTML file name of the client. For example, if you created an HTML file in the Deployment Wizard called 3270sessions.html, you can load it by specifying a URL such as the following:

  ```
  http://host.yourcompany.com/hod/3270sessions.html
  ```
- Load the HODMain_*xx*.html file, where *xx* is your two letter language suffix, into your browser to view links to all the available predefined clients. HODMain_xx.html is located in the publish directory.

When you access a client, a security warning appears to notify you that Host On-Demand was created by **International Business Machines** and to ask whether you trust it. Users must grant privileges in order for Host On-Demand to work properly.

Cached clients

A cached client is any client where you choose to cache the applet on the user's machine. It is recommended that you create cached client HTML files using the Deployment Wizard; however, you can also use the predefined cached clients supplied with Host On-Demand.

The cached client is saved (or cached) on your local disk the first time you download it. The next time you start the emulator session, only a small applet downloads from the server, reducing the time needed to start the session. The applet that is downloaded checks to see if the version of the client on the server is more recent than the one that has been cached. If so, the cached version is updated. The cached client is recommended for users with slow connectivity (such as dial-up phone lines) where downloading a large applet would take a long time.

The cached client is persistent across operating system restarts and browser reloads. If you have a cached client on your machine, you can only use other cached clients. For Java 1 browsers, you cannot use download clients until you remove the cached client. For instructions on how to delete it (for instance, if you want to load a download client), see "Removing cached clients" on page 83.

Installing cached clients

You can install a cached client from the Web server by launching a customized HTML file created by the Deployment Wizard that specifies the client is a cached client or by using the "Predefined emulator clients" on page 88. Alternatively, if you are not running a Java 2-enabled client, you can install the cached client from a local source (such as a CD or network drive).

Installing the cached client from the Host On-Demand Server

To install a cached client from the server, do one of the following:

- Specify the full URL of the HTML file in your browser, as described in "Loading emulator clients" on page 81.
- If you want to use a predefined client, click on the cached client link after loading http://*server_name*/*hod_alias*/HODMain.html, where *server_name* is the host name or IP address of the Host On-Demand server and *hod_alias* is the alias (or path) of the published directory.

The client begins installing immediately. A new browser window shows the status of the installation. The top progress bar shows the status of individual files as they download. The bottom progress bar shows the status of the overall installation. When the installation is complete, you are prompted to restart the browser.

If you are installing the cached client on a supported Java 2 browser, a separate installation progress window does not appear. Also, with these browsers, you do not need to restart the browser before using Host On-Demand.

Installing the cached client from a LAN or CD (only for Java 1 clients)

To install a customized cached client from a LAN or CD:

1. Use the Deployment Wizard to create your customized *.html and *.zip files (for example, MyHOD.html and myHOD.zip). If you need to distribute the Deployment Wizard files to another server, you might want to create the .zip output option to allow you to use DWunzip. For more information, see Using DWunzip in the online help.
2. After loading the new Deployment Wizard files to your server, test the new files to make sure they function as expected.
3. Copy or FTP the following files from the publish directory of your Host On-Demand server installation to a network drive or CD:
   - MyHOD.html
   - z_MyHOD.html (if it exists)
   - hoddetect*.html
   - hodlogo.gif
   - hodbkgnd.gif
   - Installer.html
   - *.jar
   - *.cab
   - *.properties
   - *.js

   The following files are in subdirectories of the publish directory of your Host On-Demand server installation. You must keep these files in the appropriate subdirectories when copying them to your LAN or CD drive.

   - msgs\cached_*.properties
   - com\ibm\eNetwork\HOD\detect\DetectPluginApplet.class

4. The CD must be distributed with the same guidelines as the License Agreement and Export and Import regulations because it contains encryption technology.
5. The date and timestamp of the files on the CD must match the files on the server. If they do not, the Web server may reload the files to the client machine.
6. On the client machine, point the browser to MyHOD.html on the CD to preload the cached client into the Web browser cache.
7. After loading the cached client from the CD, restart the browser and point to the MyHOD.html on the server.

Removing cached clients

To remove the cached client, load `http://` *server_name*/*hod_alias*/`HODRemove.html` in your browser.

If you are using a Java 2-enabled Web browser, a message appears instructing you to use the Java Control Panel to remove the JRE cache, where the Java files used to run the cached client on a Java 2-enabled Web browser are stored.

For more information, see “Java 2-enabled Web browsers” on page 24.

Cached client support when accessing multiple Host On-Demand servers

Java 1

If you deploy the cached client to the Internet, consider that your users might use Host On-Demand with other business partners running Host On-Demand servers at different service levels. This could be a problem if your user needs different functions when accessing servers at different service levels. Components of different service levels are not supported within a single cached client, and there can be only one cached client on a machine. Host On-Demand Version 5.0.4 or higher is required to run the cached client across the Internet.

To prevent complications, you can do some or all of the following:

- Select all the functions a user needs (across all sites the user accesses) in a preload list when you create an HTML file using the Deployment Wizard
- Use the disable function of the Deployment Wizard to disable all functions not in the preload list and the functions that are not needed for your users
- Create separate HTML files for different user groups
- Give your HTML files a name that identifies your company
- Always install Screen Customizer to prevent users who are accessing your server from losing Screen Customizer functions when accessing other sites

If the software on the server is an earlier version than the cached software, the cached client applet checks the version levels of the components and prevents caching of any new components. To cache new components, remove the more recent version of the cached client and then install the earlier version of the cached client. To avoid this problem, select all the functions the user needs (across all sites the user accesses) in the preload list when you create the HTML file using the Deployment Wizard.

When a client points to a server running a later version of Host On-Demand, *and the upgrade test passes, all* cached components are automatically upgraded (not only the components defined in the HTML file's preload list). Because all cached and new components are upgraded simultaneously, the upgrade might generate additional Web Server load. After the upgrade, the client can point back to the server running the earlier version of Host On-Demand, and the more recent cached client functions correctly.

If you use the cached client on the Internet, you must install Screen Customizer on your server. If a full function version of Screen Customizer is cached and Screen Customizer is not installed on the server, the cached client applet issues an error message and prevents the upgrade.

If you are using locally stored preferences, the custom HTML files you create must have names unique to your company, because the HTML file names differentiate between the locally stored preferences of different sites. Using generic names could cause preference conflicts for your users.

If you have problems managing cached client deployment on the Internet, see the (Host On-Demand support Web site) for more information.

Java 2

With Java 2, the clients get a separate copy of the cached client code for each Host On-Demand Server they access, so there is no problem accessing servers at different service levels. With some versions of the plug-in, users may need to increase the size of their Java 2 cache if they are going to visit many Host On-Demand Servers.

Internet Explorer cached client support for Windows 2000 and Windows XP

Java 1

Windows 2000 and Windows XP restricted users may now download the Host On-Demand cached client. Previously, only those users with Power User or Administrator authority could use the cached client.

On a multi-user Windows machine running Windows 2000 or Windows XP, each user can download their own version of the cached client. Multi-user machines running Windows NT and Windows 95/98/Me continue to have all users share one copy of the cached client. You can allow all users on a Windows 2000 or Windows XP multi-user machine to share a single instance of the cached client by adding the ShareCachedClient parameter to the applet tag of cached client HTML files through the (Additional Parameters) tab under Advanced Options.

When the cached client is shared, it is downloaded to a directory such as \Documents and Settings\All Users\IBMHOD. An Administrator or Power User must either create this directory manually or do the first install of the shared cached client. In either case, the Administrator or Power User must change the security settings for this directory so that restricted users have Read, Modify, and Write access. The Administrator can either change the security settings and then download the cached client to the directory; or download the shared cached client to the directory and then change the security settings. If the security settings are not updated and a restricted user attempts to install the shared cached client, the user receives an error message that indicates there may be a problem with the file system and the restricted user will not be able to use or update the cached client.

Once the Administrator or Power User changes the security settings, a restricted user can log on to Windows and can either install the shared cached client or use (or update) a previously installed version of the shared cached client. Other restricted users can log on to Windows and use the cached client without having to download it from the Host On-Demand server again. They can also upgrade the shared cached client, if necessary. After the shared cached client is installed, any user that logs onto Windows to use the cached client will need to restart the browser when prompted.

If you do not want restricted users to share the cached client, a separate instance of the cached client is downloaded to the user directory for each restricted user.

If the previous version of the cached client was downloaded by an Administrator or a Power User, and you want to allow restricted users to access it, an Administrator or Power User must use HODRemove.html to remove the previous version of the cached client, then change the security settings to the shared cached client directory to Read, Modify, and Write for restricted users, as described above.

Java 2

For clients running the Java 2 plug-in, the Java 2 security model prohibits sharing of the cached client files.

Troubleshooting cached clients

If you find that you cannot load the cached client, check the items described below.

Netscape 4.x

1. In the browser window, click Edit > Preferences > Advanced.
2. Check Enable Java.
3. Check Enable JavaScript.

Microsoft Internet Explorer 4.0.1

1. In the browser window, click View > Internet Options > Security.
2. Make sure that the Internet and Local Intranet zones are set to Medium security.

Microsoft Internet Explorer 5.5

After upgrading your browser from Microsoft Internet Explorer 4 to Microsoft Internet Explorer 5.5, you may receive security exceptions in the Java console. When you install the Cached Client, several files are stored into the browser's directory structure. When you upgrade Internet Explorer from Version 4 to Version 5, the browser will no longer know about the CAB files which contain the Host On-Demand cached code. Since the browser cannot find the CAB files, it tries to use the class files directly from the server, causing security exceptions. To resolve this, following a version upgrade of your browser, you should remove Host On-Demand using HODRemove.html, and then reinstall the product using HODCached.html.

Download clients

Unlike cached clients, download clients are downloaded from the Host On-Demand server every time you use them. Any client that is not cached is considered a download client. Use download clients if:

- You do not want to take up disk space on client machines by installing the cached client or the locally-installed client.
- Your initial download time is not an issue.

Launching the download client

Launch the download client by downloading it from the Host On-Demand server into your browser window, as described in "Loading emulator clients" on page 81.

Launching the download client after installing the cached client

Java 1

If you have installed a cached client and then later decide to launch a download client, you must first do the following:

1. Remove the cached client from the browser by loading HODRemove.html in your browser, as described in "Removing cached clients" on page 83.
2. Restart your browser.

If you do not remove the cached client before loading the download client, the session will not start and an error message is displayed directing you to run HODRemove.html before you can launch the download client.

Java 2

With Java 2 clients, you can successfully launch the download client after installing the cached client.

Selecting download client vs. cached client

The types of Host On-Demand clients that you use depend on your computing environment and your personal preferences.

Download clients are generally used in networked environments because high-speed network connections reduce the time it takes to download them from the Web server. They are not recommended for use over low-speed dialup connections because they need to be downloaded every time they are used, which takes more time on dialup connections. The small disk footprint of download clients is especially suited for client machines that do not have a lot of local disk space, such as NetStation machines.

Cached clients are stored locally and load faster than download clients (unless an updated version of the client is being downloaded from the Web server). They can be used equally well over network and dial-up connections. Cached clients do take up more local disk space than download clients, but on most machines this is not a problem.

Both cached and download clients can be used in the same Host On-Demand environment, although cached clients need to be deleted before a download client can be loaded. (See Chapter 12, “Using Host On-Demand emulator clients” on page 81 for instructions on how to delete cached clients.)

Regardless of whether you plan to used download clients, cached clients, or both, it is recommended that you create your own clients using the Deployment Wizard instead of using one of the predefined clients. See “Reducing client download size” on page 88 for more information.

Function On-Demand client (HODThin.html)

The Function On-Demand client is not available for Java 2-enabled Web browsers, such as Netscape 6.0.

It is strongly recommended that you use the Deployment Wizard to create a customized HTML file instead of using of the Function On-Demand client.

The Function On-Demand (`HODThin.html`) client is much smaller than the other clients. Initially, only the basic functions are downloaded, so the startup time is greatly reduced. Other functions are downloaded when they are needed. Some functions might be required immediately (such as the 3270 emulator), while other functions (file transfer, for example) might never be invoked or might not be needed for a long time.

The Function On-Demand client is downloaded from the server every time you want to use it.

Predefined emulator clients

Several predefined emulator client HTML files are supplied with Host On-Demand. They are included to demonstrate the range of Host On-Demand client functionality and serve as examples for creating customized HTML files in the Deployment Wizard. All of them use the Configuration server-based model. To load one of these clients, follow the instructions in “Loading emulator clients” on page 81.

In general, it is recommended that you define your own customized HTML files with the Deployment Wizard instead of using the predefined client HTML files.

The following predefined emulator client HTML files are provided by Host On-Demand:

There is a delay using predefined HTML files if you use Internet Explorer only with Java 1. To avoid this delay, you can edit the HTML and change the hod_JavaType JavaScript variable from a value of ’detect’ to ’java1’.

Cached client (HODCached.html)
Provides all Host On-Demand client functions and the Screen Customizer.

Cached client with problem determination (HODCachedDebug.html)[1]
Starts the cached client with problem determination (session logging and tracing).

Download client (HOD.html)
Provides all Host On-Demand client functions except problem determination.

Accessing HOD.html with a Java 2 browser works with limited functions. For a list of functions that do not work, see “Limitations for Host On-Demand” on page 24. Loading HODDebug.html instead results in full functionality for Host On-Demand. However, the hoddbg.jar file that is downloaded is approximately 4.5 MB.

Download client with problem determination (HODDebug.html)[1]
Loads the download client with problem determination (session logging and tracing).

Function On-Demand client (HODThin.html)
Provides only the Host On-Demand basic client functions.

Notes:

1. Use the problem determination clients only if you are working with Support to resolve a problem with your Host On-Demand installation.

Reducing client download size

In general, it is a good idea to keep the size of your Host On-Demand clients (whether download or cached clients) as small as possible. This speeds up their download time and conserves disk space on the client machine.

The best way to minimize the size of your Host On-Demand clients is to create them using the Deployment Wizard. The predefined clients supplied with Host On-Demand are typically larger than the custom clients created with the Deployment Wizard because they contain Host On-Demand’s full range of client functionality. Clients created in the Deployment Wizard contain only the functions that you select to be pre-installed. In addition, Deployment Wizard clients are downloaded in compressed format. This further reduces their download size.

When you create a customized client with the Deployment Wizard, you can select only the functions that you know users are going to need on the Preload Options panel in the Deployment Wizard. For instance, if your users are only going to need 3270 terminal and 3270 printer sessions, do not select any other session types when you are creating the client in the Deployment Wizard. Including support for unused session types increases the size of the client without improving its functionality. You can also choose not to download components for functions that are not frequently used. Unless you choose to disable that function in the Deployment Wizard, users will be prompted to download any necessary components when they use that function. If you need additional session types later, you don't necessarily have to create a new client type. You can add the new session types to the preload list on the Preload Options panel instead.

Do not use debugging or problem determination in either Deployment Wizard-generated or predefined clients. This greatly increases the size of the client and can slow down a client's performance. Debugging and problem determination clients are not intended for general use. Use them only in conjunction with Host On-Demand technical support to diagnose and solve problems with your Host On-Demand system.

Chapter 13. Using Database On-Demand clients

Database On-Demand is a Java applet that allows users to perform Structured Query Language (SQL) requests to iSeries databases through a JDBC driver. Database On-Demand is shipped with a JDBC driver for the iSeries. Other user-installed JDBC drivers can be registered and used, although IBM does not provide support for these drivers.

Features of Database On-Demand include:

- A graphical interface to aid in constructing SQL statements and File Upload statements
- The ability to display on screen the results of the executable statements you build, to save the results of SQL statements in various file formats and to upload entire files in various formats to a host database
- The ability to create dynamic queries, using the graphical interface, that can be executed or saved for later use

You cannot create Database On-Demand clients using the Deployment Wizard. Database On-Demand clients are only available using the predefined clients.

For more Database On-Demand overview information, see Database On-Demand in the Host On-Demand online help.

Loading Database On-Demand clients

To load a Database On-Demand client, do one of the following:

- Specify the full URL of the HTML file in your browser:

  ```
  http://server_name/hod_alias/client_name.html
  ```

  where *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_name* is the HTML file name of the Database On-Demand client. For example, you can load the download version of the Database On-Demand client from the Web server by specifying a URL such as the following:

  ```
  http://host.yourcompany.com/hod/HODDatabase.html
  ```
- Load the HODMain_*xx*.html file, where *xx* is your two letter language suffix, into your browser to view links to all the available Database On-Demand clients, plus other predefined clients. HODMain_xx.html is located in the publish directory.

If you use Database On-Demand on Windows 2000 with Netscape 6.x, your machine should have more than 128 MB of memory.

Database On-Demand clients

Host On-Demand supplies the following predefined Database On-Demand clients:

There will be a delay using predefined HTML files if you use Internet Explorer only with Java 1. To avoid this delay, you can edit the HTML and change the hod_JavaType JavaScript variable from a value of ’detect’ to ’java1’.

Database On-Demand client (HODDatabase.html)

Provides users with a means of making Structured Query Language (SQL) requests to iSeries databases through a Java database connectivity (JDBC) driver. Users can save the results of their requests and use them in other applications, such as a spreadsheet.

Database On-Demand client cached (HODDatabaseCached.html)

This client starts the Database On-Demand client in a cached environment. The advantage of the Database On-Demand cached client is that it can be cached along with the Host On-Demand cached client in the browser.

If your client is going to use multiple code pages, you need to add the appropriate archive (.jar/.cab) file of each code page to the preload list of your cached HTML. For a list of code-page languages and corresponding file names, see "Using multiple code pages with Database On-Demand".

Database On-Demand client cached with problem determination (HODDatabaseCachedDebug.html)

This client starts the Database On-Demand client in a cached environment with problem determination. Load this HTML file if you want to use the Database On-Demand client in cached environment with problem determination (session logging and tracing).

Use the problem determination client only if you are working with Support to resolve a problem with your Host On-Demand installation.

Setting up Database On-Demand users

To configure users so they can access Database On-Demand, you must first define groups and users in the Host On-Demand configuration server. Then you can define the database functions that groups and users can perform and later manage the statements that users have created. The administrator cannot create SQL statements for users.

If you are using Database On-Demand with Netscape 4.x, you must turn the Just In Time (JIT) compiler off. Unfortunately, due to problems found with the JIT compiler, this means that you cannot take advantage of both the Database On-Demand and integrated Windows domain logon functions.

For more detailed information about setting up groups and users to access Database On-Demand, see the topics Getting started with Database On-Demand and Setting up options for Database On-Demand users in the Host On-Demand online help.

Using multiple code pages with Database On-Demand

If you wish to use multiple code pages with Database On-Demand, you must add jar or cab files to your HTML file. Only those code pages that correspond to the language of the HTML file are automatically loaded. For example, if you are running from a French computer, but you want to access a Dutch host, you must make these modifications.

Edit the CommonJars.js file. If you are using a download client, look for the line that starts "dbaDownloadJars =" and add the appropriate file names from the table below. Use jar file names, even if your clients will be using Internet Explorer (the names will be converted to cab file names later). If you are using a cached client, look for the line that starts “dbaCachedComps =” and add the appropriate component name from the table below.

Supported Database On-Demand code pages

The following table lists the supported Database On-Demand client code-page languages, the corresponding .jar file names, and the cached component names:

Code-page language	.JAR file name	Component name
Arabic	hacpar.jar	HACPAR
Czech, Hungarian, Polish, Slovenian	hacpce.jar	HACPCE
Danish, Finnish, Dutch, Norwegian, Swedish	hacp1b.jar	HACP1B
German, Spanish, French, Italian, Portuguese, Brazilian Portuguese	hacp1a.jar	HACP1A
Greek	hacpgr.jar	HACPGR
Hebrew	hacphe.jar	HACPHE
Japanese	hacpja.jar	HACPJA
Korean	hacpko.jar	HACPKO
Russian	hacpru.jar	HACPRU
Simplified Chinese	hacpzh.jar	HACPZH
Thai	hacpth.jar	HACPTH
Turkish	hacptr.jar	HACPTR
Traditional Chinese	hacptw.jar	HACPTW

Chapter 14. Modifying session properties dynamically

Host On-Demand sessions are defined by the administrator and retrieved by the Host On-Demand client when a user accesses a Host On-Demand HTML file. The session properties a user sees are fixed values and consist of a combination of the administrator's initial configuration and any user updates. However, there may be times when it would be useful with some HTML files, or with certain session properties, to dynamically set a value at the time that the HTML is accessed. This type of control allows you to set particular session property values based on information such as the IP address of the client or the time of day.

In order to dynamically set session properties at the time the HTML is accessed, the administrator must write a program that runs on the Web server and effectively modifies the HTML just before it is sent to the client. Even though the initial session properties are not defined in the HTML, Host On-Demand provides the capability to override many of the session properties in the HTML. These override values are always used by the client and take precedence over both the initial session properties setup by the administrator, as well as any updates for the property made by the user. The HTML override value is never stored, so the client will return to using prior settings for the property whenever the administrator removes the override. Also, the overridden property is locked so a user cannot change it.

There are many ways in which an administrator could write a program to dynamically set one or more session properties using the HTML overrides, such as using Java Server Pages (JSP), servlets, Perl, REXX, or Active Server Pages (ASP). This chapter takes you through a couple of examples that focus on common administrator issues. These examples are meant to demonstrate the syntax and technique of overriding particular properties. These mechanisms apply to whichever programming approach the administrator may choose.

Setting up the initial HTML

The initial HTML should be created using the Deployment Wizard, which will allow you to set up the features that are important to you, such as the size of the downloaded code and the functions available to your users. It will also help you by generating HTML that is correctly formatted for the client Java level you wish to support. The following sections describe the HTML parameters you will need to include. However, keep in mind that the exact format required for these parameters will vary depending on the format of the HTML, which, in turn, depends on the client Java level supported. Examples using both formats (Java 1 and Java 2/Auto Detect) are shown at the end of this chapter. Note that in Host On-Demand 7, some of the HTML is generated using JavaScript, and HTML parameters are specified within a JavaScript array or using JavaScript document.write statements. Also, the format of the HTML varies according to the Java type (Java 1, Java 2, or Auto Detect) selected and whether the cached or download client is selected.

Overriding HTML parameters

There are several steps you must follow in order to dynamically set session properties (the examples shown later in this chapter will help clarify how some of these parameters should be specified):

1. **Enable HTML overrides**. By default, the client will ignore HTML overrides. To enable overrides, you will need to include an HTML parameter called EnableHTMLOverrides and set it to a value of true.
2. **List the sessions to be overridden**. Because there may be multiple sessions associated with an HTML, you will need to list which ones will be overridden. You will need to include an HTML parameter called TargetedSessionList, having a value of the exact names of the sessions that should accept overrides. The value should be a comma-separated list of session names, such as ″Session1Name, Session2Name″.
3. **Specify the override itself**. For each session property to be overridden, you will need to include an HTML parameter called the property name, with the value being the desired override. The value you specify will then apply to all sessions listed in your TargetedSessionList parameter. If you wish to only override a subset of the sessions in your TargetedSessionList, you can specify a value in the format of ″Session1Name=value1, Session2Name=value2″, for example.

Specific session properties that can be overridden

The following table describes the session properties that can be overridden and gives the acceptable values for each parameter:

Table 11. Session properties that can be overridden

Parameter name	Description	Valid values
Host	Host name or IP address of the target server. Appears as ″Destination address″ on property panels. Applies to all session types.	Host name or IP address.
Port	The port number on which the target server is listening. Appears as ″Destination port″ on property panels. Applies to all session types.	Any valid TCP/IP port number.
CodePage	The codepage of the server to which the session will connect. Appears as ″Host Code-Page″ on property panels. Applies to all session types except FTP.	The numeric portion (for example, 037) of the supported host codepage listed in the session property panel.
SessionID	The short name you want to assign to this session (appears in the OIA). It must be unique to this configuration. Appears as ″Session ID″ on property panels. Applies to all session types.	One character: A-Z.

Table 11. Session properties that can be overridden (continued)

Parameter name	Description	Valid values
LUName	The name of the LU or LU Pool, defined at the target server, to which you want this session to connect. Appears as ″LU or Pool Name″ on property panels. Applies to 3270 Display and 3270 Printer session types.	The name of an LU or LU Pool.
WorkstationID	The name of this workstation. Appears as ″Workstation ID″ on property panels. Applies to 5250 Display and 5250 Print session types.	A unique name for this workstation.
ScreenSize	Defines the number of rows and columns on the screen. Appears as ″Screen Size″ on property panels. Applies to 3270 Display, 5250 Display, and VT Display session types.	• value=rows x columns • 2=24x80 (3270, 5250, VT) • 3=32x80 (3270) • 4=43x80 (3270) • 5=27x132 (3270, 5250) • 6=24x132 (VT) • 7=36x80 (VT) • 8=36x132 (VT) • 9=48x80 (VT) • 10=48x132 (VT) • 11=72x80 (VT) • 12=72x132 (VT) • 13=144x80 (VT) • 14=144x132 (VT) • 15=25x80 (VT) • 16=25x132 (VT)
SLPScope	Service Location Protocol (SLP) Scope. Appears as ″Scope″ under ″SLP Options″ on property panels. Applies to 3270 Display, 3270 Printer, 5250 Display, and 5250 Printer session types.	Contact your administrator to get the correct value for this field.
SLPAS400Name	Connects a session to a specific iSeries. Appears as ″AS/400 Name (SLP)″ on property panels. Applies to 5250 Display and 5250 Printer session types.	The fully-qualified SNA CP name (for example, USIBMNM.RAS400B).

Table 11. Session properties that can be overridden (continued)

Parameter name	Description	Valid values
SSLCertificateSource	The certificate can be kept in the client's browser or dedicated security device, such as a smart card; or, it can be kept in a local or network-accessed file. Appears as ″Certificate Source″ on property panels. Applies to 3270 Display, 3270 Printer, 5250 Display, 5250 Printer, and VT Display session types.	The value is SSL_CERTIFICATE_IN_CSP for a certificate in a browser or security device. The value is SSL_CERTIFICATE_IN_URL for a certificate in a URL or file.
SSLCertificateURL	Specifies the default location of the client certificate. Appears as ″URL or Path and Filename″ in property panels. Applies to 3270 Display, 3270 Printer, 5250 Display, 5250 Printer, and VT Display session types.	The URL protocols you can use depend on the capabilities of your browser. Most browsers support HTTP, HTTPS, FTP, and FTPS.
FTPUser	Specifies the user ID the session uses when connecting to the FTP server. Appears as ″User ID″ on property panels. Applies to FTP session types.	A valid user ID.
FTPPassword	Specifies the password the session uses when connecting to the FTP server. Appears as ″Password″ on property panels. Applies to FTP session types.	A valid password.
UseFTPAnonymousLogon	Enables the session to log in to an FTP server using anonymous as the user ID. Appears as ″Anonymous Login″ on property panels. Applies to FTP session types.	Yes or No.
FTPEmailAddress	Specifies the e-mail address to use when connecting to the FTP server while using Anonymous Login. Appears as ″E-mail Address″ on property panels. Applies to FTP session types.	A valid e-mail address.

Table 11. Session properties that can be overridden (continued)

Parameter name	Description	Valid values
Netname	The name of the terminal resource to be installed or reserved. If this field is blank, the selected terminal type is not predictable. Applies to CICS sessions only.	A valid terminal resource name.

Any errors encountered in processing the HTML parameters is displayed in the Java console.

Example #1: Overriding the LU name based on the client's IP address

Administrators may want to avoid specifying LU names directly in session definitions. This example shows a simple way of using the IP address of the client to look up an LU name listed in a text file and use it as an override value in a session.

This example is written using JSP. The Deployment Wizard was used to create an HTML file that contains two sessions named 3270 Display and 5250 Display. Note that in Host On-Demand 7, some of the HTML is generated using JavaScript, and HTML parameters are specified within a JavaScript array or using JavaScript document.write statements. Also, the format of the HTML varies according to the Java type (Java 1, Java 2, or Auto Detect) selected and whether the cached or download client is selected. In this example, a Java 1 cached client was selected.

A file (c:\luname.table) is read that contains IP address/LU name pairs. The IP address of the client is used to look up the proper LU name, which is overridden in the ″3270 Display″ session. See the comments in the example for more detail. The lines added to the Deployment Wizard output are displayed in **bold**.

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<%
//  Read the luname.table file into a properties variable.
//  The luname.table file contains lines in the following format:
//    ipaddress=luname
Properties lunames = new Properties();
lunames.load(new FileInputStream("c:\\luname.table"));
%>
<!-- HOD WIZARD HTML -->
<HTML>
<HEAD>
<META content="text/html; charset=UTF-8">
<!-- TITLE Begin -->
<TITLE>Example1</TITLE>
<!-- TITLE End -->
<!-- SUMMARY Begin -->
<!--
Configuration Model
 What configuration model would you like to use?
 -HTML-based model
Sessions created
 -3270 Display
 -5250 Display
Additional Options
 -Allow users to save session changes? = True
 -Cached = True
 -Java Type = java1
```

```
Disable Functions
Preload Options
 -5250 Sessions = True
 -Change Session Properties = True
 -FTP Sessions = True
 -3270 Sessions = True
Server Connection Options
Cache Options
 Basic Options
 -Debug = False
 -Height (in pixels) = 250
 -Width  (in pixels) = 550
 Cache Client Upgrade Option
 -Percent of users who can upgrade by default = 100
 -Prompt user (user decides foreground or background)
Advanced Options
 Display
 -Standard Host On-Demand Client
 -Applet size = Autosize to browser
 -Maximum sessions = 26
 Other
 -Locale = Use the system Locale
 -Debug = False
 -HTML Template = Default
 Additional Parameters
 -None
-->
<!-- SUMMARY End -->
</HEAD>

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

<SCRIPT LANGUAGE="JavaScript">
function writeAppletParameters()
{
   document.write("");
}
</SCRIPT>

<SCRIPT LANGUAGE="JAVASCRIPT" SRC="CachedJ1.js"></SCRIPT>
<SCRIPT LANGUAGE="JAVASCRIPT">
var hod_Height='80%';
var hod_Width='80%';
document.write('<APPLET ARCHIVE="CachedAppletSupporter.jar" MAYSCRIPT
NAME="HODApplet"
CODE="com.ibm.eNetwork.HOD.cached.appletloader.CachedAppletLoader"
WIDTH="'+hod_Width+'" HEIGHT="'+hod_Height+'">');
document.write('<PARAM NAME="Cabinets"
VALUE="CachedAppletSupporter.cab">');
document.write('<PARAM NAME="CachedClient"            VALUE="true">');
document.write('<PARAM NAME="ParameterFile"
VALUE="HODData\\Example1\\params.txt">');
document.write('<PARAM NAME="JavaScriptAPI"           VALUE="false">');

// The next 2 lines are required in order to override session properties.
//  The first line turns on the processing for this function and does not
//  need to be modified.  The second line identifies the sessions that you
//  want to change.  In this example, there are 2 sessions identified
//  named: "3270 Display" and "5250 Display".

document.write('<PARAM NAME="EnableHTMLOverrides" VALUE="true">');
document.write('<PARAM NAME="TargetedSessionList"
    VALUE="3270 Display,5250 Display">');
```

```
// The following line changes the LUName session parameter for the session named
//  "3270 Display".  In this example, the LUName is being set to the value
//  contained in the c:\luname.table for the IP address of the client.
//  When you are initially testing your changes, you may want to use a constant
//  value to verify that the syntax is correct before you insert your
//  calculations.
document.write('<PARAM NAME="Luname" VALUE="3270
Display=<%=lunames.get(request.getRemoteAddr())%>">');

writeAppletParameters();
document.write("</APPLET>");
</SCRIPT>

<P>
<SCRIPT LANGUAGE="JavaScript">
var hod_AppName='';
var hod_Preloadlist='HABASE;HODBASE;HODIMG;HACP;HAFNTIB;
    HAFNTAP;HA3270;HODCFG;HAFTP;HA5250';
var hod_Debugcomponents='false';
var hod_Debugcachedclient='false';
var hod_Upgradepromptresponse='Prompt';
var hod_Upgradepercent='100';
var hod_Framewidth='550';
var hod_Frameheight='250';

function isBookmark(mySearch) {
  if (mySearch.length < 2) {
    return false;
  } else {
    return (mySearch.toLowerCase().indexOf('launch=') != -1);
  }
}

if (hod_AppName == '') {
  if (isBookmark(window.location.search.substring(1)))
    hod_AppName = 'com.ibm.eNetwork.HOD.SessionLauncher';
  else
    hod_AppName = 'com.ibm.eNetwork.HOD.HostOnDemand';
}

function getHODFrame() {
  return self;
}

document.write('<APPLET ARCHIVE="CachedAppletSupporter.jar" MAYSCRIPT
NAME="CachedAppletSupporter"
CODE="com.ibm.eNetwork.HOD.cached.appletsupport.CachedAppletSupportApplet"
WIDTH="2" HEIGHT="2">');
document.write('<PARAM NAME="Cabinets"
VALUE="CachedAppletSupporter.cab">');
document.write('<PARAM NAME="DebugComponents"
VALUE="'+hod_Debugcomponents+'">');
document.write('<PARAM NAME="PreloadComponentList"
VALUE="'+hod_Preloadlist+'">');
document.write('<PARAM NAME="DebugCachedClient"
VALUE="'+hod_Debugcachedclient+'">');
document.write('<PARAM NAME="CachedClientSupportedApplet"
VALUE="'+hod_AppName+'">');
document.write('<PARAM NAME="InstallerFrameWidth"
VALUE="'+hod_Framewidth+'">');
document.write('<PARAM NAME="InstallerFrameHeight"
VALUE="'+hod_Frameheight+'>"');
document.write('<PARAM NAME="UpgradePromptResponse"
VALUE="'+hod_Upgradepromptresponse+'">');
document.write('<PARAM NAME="UpgradePercent"
VALUE="'+hod_Upgradepercent+'">');
document.write('</APPLET>");
```

```
</SCRIPT>

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

Example #2: Allowing the user to specify the host to connect to using an HTML form

Administrators may also want to use HTML forms to specify override values rather than calculating them. The following example displays a simple form for entry of a host name. The form posts to a JSP program which uses the host name specified in the form to override the host name in the 3270 Session.

This example is written using JSP. The Deployment Wizard was used to create an HTML file that contains two sessions named ″3270 Display″ and ″5250 Display.″ Note that in Host On-Demand 7, some of the HTML is generated using JavaScript, and HTML parameters are specified within a JavaScript array or using JavaScript document.write statements. Also, the format of the HTML varies according to the Java type (Java 1, Java 2, or Auto Detect) selected and whether the cached or download client is selected. In this example, a Java Detect download client was selected.

When using forms, the form data needs to be retained across requests to the program. This is because Host On-Demand HTML files reload themselves for Java detection and for bookmarking support when using configuration server-based model pages. If Java 1 is selected and bookmarking support is disabled if using the configuration server-based model, the page will not need to reload and there is no need to retain the form data. This example uses a JSP session to store the form data across reloads.

Here is a simple HTML form that allows for entry of a host name. The form posts to the JSP program (example2.jsp):

```
<form method="POST"  action="hod/example2.jsp">
Hostname <input name="form.hostname"><br>
<input type="submit">
</form>
```

Here is the modified output from the Deployment Wizard. See the comments in the example for more detail. The lines added to the Deployment Wizard output are displayed in **bold**.

```
<%
//  Get a session or create if necessary and store the hostname
//   entered in the form in the session.
HttpSession session = request.getSession(true);
String hostname = request.getParameter("form.hostname");

if (hostname!=null) {
    session.putValue("session.hostname", hostname);
}
%>
<HTML>
<!-- HOD WIZARD HTML -->
<HEAD>
<META content="text/html; charset=UTF-8">
<TITLE>example2</TITLE>
<!-- SUMMARY Begin -->
<!--
Configuration Model
```

```
 What configuration model would you like to use?
 -HTML-based model
Sessions created
 -3270 Display
 -5250 Display
Additional Options
 -Allow users to save session changes? = True
 -Cached = False
 -Java Type = detect
Disable Functions
Preload Options
 -5250 Sessions = True
 -Change Session Properties = True
 -3270 Sessions = True
Server Connection Options
Cache Options
Advanced Options
 Display
 -Standard Host On-Demand Client
 -Applet size = Autosize to browser
 -Maximum sessions = 26
 Other
 -Locale = Use the system Locale
 -Debug = False
 -HTML Template = Default
 Additional Parameters
 -None
-->
<!-- SUMMARY End -->
</HEAD>
<SCRIPT LANGUAGE="JAVASCRIPT" SRC="CommonJars.js"></SCRIPT>
<SCRIPT LANGUAGE="JAVASCRIPT" SRC="HODJavaDetect.js"></SCRIPT>
<SCRIPT LANGUAGE="JAVASCRIPT" SRC="CommonParms.js"></SCRIPT>
<SCRIPT LANGUAGE="JAVASCRIPT">

//---- Start JavaScript variable declarations ----//
var hod_Locale = '';
var hod_AppName ='';
var hod_AppHgt = '80%';
var hod_AppWid = '80%';
var hod_CodeBase = '';
var hod_FinalFile = 'z_example2.html';
var hod_JavaType = 'detect';
var hod_Obplet = '';
var hod_jars =
'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hodsignn.jar,
     ha3270n.jar,hodcfgn.jar,ha5250n.jar';

var hod_URL = new String(window.location);
var hod_DebugOn = false;
var hod_SearchArg = window.location.search.substring(1);

var hod_AppletParams = new Array;
hod_AppletParams[0] = '<PARAM NAME="ParameterFile"



hod_AppletParams[0] = '<PARAM NAME="ParameterFile"
     VALUE="HODData\\example2\\params.txt">';
hod_AppletParams[1] = '<PARAM NAME="ShowDocument"  VALUE="_parent">';
hod_AppletParams[2] = '<PARAM NAME="JavaScriptAPI" VALUE="false">';
hod_AppletParams[3] = '<PARAM NAME="PreloadComponentList"
VALUE="HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HA3270;HODCFG;HA5250">';

// The next 2 lines are required in order to override session properties.
//  The first line turns on the processing for this function and does not
//  need to be modified.  The second line identifies the sessions that you
//  want to change.  In this example, there are 2 sessions identified
//  named: "3270 Display" and "5250 Display".
//  Be careful to increment the array index correctly.

hod_AppletParams[4] = '<PARAM NAME="EnableHTMLOverrides" VALUE="true">';
hod_AppletParams[5] = '<PARAM NAME="TargetedSessionList"
    VALUE="3270 Display,5250 Display">';

// The following line changes the Host or Destination Address session parameter
//  for the session named "3270 Display". In this example, the Host is being set
//  to the value saved in the JSP session from the HTLM form.
//  When you are initially testing your changes, you may want to use a constant
//  value to verify that the syntax is correct before you insert your
//  calculations.

// Here we override the host for the 3270 session to the value saved in the
//  jsp session from the html form.
hod_AppletParams[6] = '<PARAM NAME="Host" VALUE="3270
    Display=<%=session.getValue("session.hostname")%>">';

var lang = detectLanguage(hod_Locale);

function getHODMsg(msgNum) {
  return HODFrame.hodMsgs[msgNum];
}
//---- End JavaScript variable declarations ----//

function getHODFrame() {
  return HODFrame;
}

document.writeln('<FRAMESET cols="*,10" border=0 FRAMEBORDER="0">');
document.writeln('<FRAME    src="hoddetect_' + lang + '.html" name="HODFrame">');
document.writeln('</FRAMESET>');
</SCRIPT>
</HEAD>
</HTML>
```

Chapter 15. Configuring Host On-Demand on zSeries

This chapter concentrates on two specific scenarios for configuring Host On-Demand on a zSeries system:

- Installing, configuring, and using the Host On-Demand configuration servlet in the WebSphere Application Server environment to communicate between Host On-Demand clients and the Host On-Demand Service Manager.
- Setting up separate read/write private and publish directories.

These configuration scenarios have several purposes:

- They provide instructions for common zSeries configuration tasks.
- They gather information on multiple products in one place, making it easier for users to perform complex configuration tasks.
- They show how Host On-Demand interacts with other WebSphere products, such as WebSphere Application Server.

See the product installation documentation (found in the Program Directory) for detailed instructions on setting up Host On-Demand on zSeries. For more information on the products involved in these configuration scenarios, see the product documentation, IBM Redbooks, and other product-related material.

Installing and configuring the Host On-Demand configuration servlet

By default, the Host On-Demand clients use port 8999 to access configuration information from the Service Manager. If any of your clients are outside the firewall, the firewall administrator needs to open port 8999 both internally and externally. However, with Host On-Demand you can avoid opening this port by customizing your clients to use the configuration servlet to access configuration information. It can be configured to run either from the WebSphere Application Server HTTP server plug-in or from the WebSphere Application Server Web container.

The steps required to configure Host On-Demand are as follows:

1. Set up the zSeries system and install Host On-Demand, WebSphere Application Server 4.0.1, and the IBM HTTP server.
2. Modify the HTTP server configuration file.
3. Set up the HTTP server environment variables.
4. Decide whether you want the configuration servlet to run from the WebSphere Application Server version 4.0 plug-in or the WebSphere Application Server version 4.0 Web container, and install it accordingly.
5. Enable clients to use the configuration servlet.
6. Restart the HTTP server and the Host On-Demand Service Manager.
7. Verify that the configuration servlet is enabled.

If you receive the following error when starting the Service Manager:

```
remote.Server. : Server Socket Contructor Failed:EDC81151 Address already in use.
***Error - Failed to start Service Manager on port 8999
```

check in the BPXPRMxx member of SYS1.PARMLIB or the PARMLIB (which contains the BPXPRMxx member) to see if the INADDRANYPORT and INADDRANYCOUNT parameters have a port range that includes 8999. If so, change the port range to exclude 8999 for Host On-Demand. Refer to *MVS Initialization and Tuning Reference, SC28–1752* for more information about BPXPRMxx and the INADDRANYPORT and INADDRANYCOUNT parameters.

Set up the zSeries system

Before you start configuring Host On-Demand, you need to set up the zSeries system.

1. Verify that the following are installed:
   - OS/390 V2R10, z/OS V1.1 or later
   - The Communication Server package that is shipped with the operating system
2. Install WebSphere Application Server version 4.0.1 and run the installation verification program (IVP). See “WebSphere Application Server 4.0.1 requirements” for more information.
3. Install the IBM HTTP server version 5.3.
4. Install Host On-Demand 7

WebSphere Application Server 4.0.1 requirements

WebSphere Application Server version 4.0.1 has the following requirements:

- Workload management (WLM). See the IBM Redbook *Prepare OS/390 for WebSphere Enterprise Edition* (part number SG24–5685–00), available at www.redbooks.ibm.com. Follow the instructions in chapter 2 to set up a monoplex and chapter 3 to set up workload management and switch into GOAL mode.
- System logger. Follow the setup instructions in chapter 4 of *Prepare OS/390 for WebSphere Enterprise Edition*.
- Resource recovery service (RRS). Follow the setup instructions in chapter 5 of *Prepare OS/390 for WebSphere Enterprise Edition*.
- IBM DB2 relational database, 7 release 1. See the *DB2 UDB for OS/390 and zOS V7 Installation Guide* (part number GC26–9936–01). Follow the instructions in the ″Installing, migrating, and updating system parameters″ and ″Installing the DB2 subsystem″ chapters to set up DB2.
- LDAP. (WebSphere Application Server customization leads you through the required LDAP configuration steps.)
- Java 1.3

After installing WebSphere Application Server, run the IVP. In this scenario, you will be using one of the application servers (BBOASR2) that is set up as part of the IVP. For more information on installing WebSphere Application Server and running the IVP, see the *WebSphere Application Server version 4.0.1 for z/OS and OS/390 Installation and Customization Guide* (part number GA22–78834–02). Follow all instructions for running the installation CLIST and configuration jobs, and complete the IVP.

Tips for configuring WebSphere Application Server: The following tips can help you to successfully configure WebSphere Application Server 4.0.1:

- Increase the BP32K buffer pools in DB2 to at least 100.
- Set up 32K temporary work files in DB2.
- Run WLM in goal mode. To find out whether your zSeries system is running WLM in this mode, enter the following command from the z/OS or OS/390 system console:

  ```
  d wlm,systems
  ```

  If the system is not in goal mode, enter the following command:

  ```
  modify wlm,mode=goal
  ```
- Make sure that the following WLM application environments are available:
  - CBSYSMGT
  - CBNAMING
  - CBINTFRP
  - BBOASR2

  To view the available environments, issue the following command from the z/OS or OS/390 system console:

  ```
  display wlm,applenv=*
  ```

  If one of the previous environments is not available (for example, CBSYSMGT), issue the following command:

  ```
  vary wlm,applenv=CBSYSMGT,resume
  ```
- Before running the job BBOCBGRT, define the DSNJDBC plan by running the DB2 job DSNTJJCL.
- Before running the job BBOLD2DB, verify that the LDAP module is included in the link list and is APF authorized. (For example, the module was 'GLD.SGLDLNK' on our test system.)
- If you have problems bringing up the BBOASR2 application server defined in the WAS 4.0.1 IVP, do the following:
  - Add /usr/lib to the classpaths for the BBOASR2 server and the CBSYSMGT server.
  - Remove /usr/lib from the classpath for the CBNAMING server.
- Verify that the host.default_host.alias value in your was.conf file is correct for your system.

Modify the HTTP server configuration file

After you have verified that the system has been set up correctly, add the following lines to the HTTP Web server config file /etc/httpd.conf:

- The servlet initialization statement:

  ```
  ServerInit /usr/lpp/WebSphere/WebServerPlugIn/bin/was400plugin.so:init_exit
     /usr/lpp/WebSphere,/config_dir/was.conf
  ```

  where *config_dir* is the directory where the was.conf file is stored. This statement must be on one line in the /etc/httpd.conf file. You also need to verify that the host.default_host.alias value in the was.conf file is correct for your system.
- The service statement for the configuration servlet:

  ```
  Service/HodConfig/*
       /usr/lpp/WebSphere/WebServerPlugIn/bin/was400plugin.so:service_exit
  ```

This statement must be on one line in the /etc/httpd.conf file.

Set up the HTTP server environment variables

Set the values of the following environment variables in the file /etc/httpd.envars:

Table 12. zSeries HTTP server environment variables

Environment variable	**Value**
JAVA_HOME	Set this variable to the location of the SDK home directory. For example: /usr/lpp/java/IBM/1.3
NLSPATH	Add the following directory to this variable: /usr/lpp/WebSphere/WebServerPlugIn/msg/%L/%N
LIBPATH	Add the following directory to this variable: /usr/lpp/WebSphere/wc/lib
CLASSPATH	Add the following directory to this variable: /usr/lpp/WebSphere/wc/lib

See the WebSphere Application Server 4.0.1 IVP instructions for detailed explanations of these environment variables.

Install the configuration servlet

You have two options for installing the configuration servlet:

- Install the configuration servlet to be run from the WebSphere Application Server version 4.0.1 Web container. Use this option if you are setting up a new WebSphere Application Server environment or would like to migrate an existing environment to the new Web container. See “Installing and running the configuration servlet from the Web container” for instructions.
- Install the configuration servlet to be run from the WebSphere Application Server version 4.0 HTTP server plug-in (which is part of the version 4.0.1 plug-in). Use this option if you would like to preserve an environment previously set up for version 3.5 of WebSphere Application Server (for example, for migration purposes). See “Installing and running the configuration servlet from the plug-in” on page 110 for instructions.

Because you cannot configure both the version 4.0 plug-in and the version 4.0.1 Web container in the same Web server, you can only select one of these options. For more detailed information on how to select an installation option, see the white paper *WebSphere Application Server V4.0 and V4.0.1 for zOS and OS/390 Configuring Web Applications* (WP100238), available from http://www.ibm.com/support/techdocs.

Installing and running the configuration servlet from the Web container

Installing and running the configuration servlet from the Web container is a two-part process:

1. Use the WebSphere Application Assembly Tool (AAT) to configure the cfgservlet.ear file (which contains the configuration servlet) for the Web container.
2. Use the WebSphere Administration Tool to install the cfgservlet.ear file in the Web container.

Configuring the cfgservlet.ear file with the AAT: Use the AAT to install the configuration servlet as follows:

1. Download the file /usr/lpp/HOD/hostondemand/lib/cgfservlet.ear in binary to your Windows system.
2. If it is not already installed on your system, download the AAT from the Web site http://www.ibm.com/software/webservers/appserv/. Click on Download and scroll for the link to WebSphere Application Server V4.0 for z/OS and OS/390 downloads. Select the AAT and follow the instructions to download and install it.
3. Launch the AAT.
4. Import the cgfservlet.ear file.
5. In the AAT window, expand Host On-Demand Configuration Servlet > Web Apps > cfgservlet.war > Web Components.
6. Select HOD Config Servlet, click the right mouse button, and select Modify.
7. Select the Parameters tab.
8. Modify the following parameters:

   ShowStats
   True

   Trace True

   ConfigServerPort
   8999 (the default). If you want the configuration servlet to use a different port than the default, change this value.
9. Save your changes.
10. Select Host On-Demand Configuration Servlet, click the right mouse button, and select Validate.
11. Select Host On-Demand Configuration Servlet > Deploy to prepare the application for export.
12. Select Host On-Demand Configuration Servlet > Export to regenerate the cfgservlet.ear file.

Install the cfgservlet.ear file with the WebSphere Application Server Administration Tool: To install the cfgservlet.ear file in the Web container, do the following:

1. Download and install the most current version of the WebSphere Application Server Administration Tool for zSeries from your server's WebSphere Application Server /bin directory (for example, /usr/lpp/WebSphere/bin/bboninst.exe).
2. Launch the WebSphere Application Server Administration Tool for zSeries.
3. Create a new conversation named HODConfig Servlet and save it.
4. Expand HODConfig Servlet > Sysplexes > *sysplex* > J2EE Servers > BBOARS2, where *sysplex* is the name of your sysplex.
5. Click the right mouse button on BBOARS2 and select Install J2EE Application.
6. Select the cfgservlet.ear file (use the Browse button if necessary).
7. Click Set the Default JNDI Path, then click OK.
8. Expand BBOASR2 > J2EEApplications. You should see Host On-Demand Configuration Servlet.
9. Select HODConfig Servlet, click the right mouse button, and select Validate.
10. Select HODConfig Servlet, click the right mouse button, and select Commit to commit the conversation.
11. Select HODConfig Servlet, click the right mouse button, and select Complete, All Tasks. Click Yes.

12. Use the z/OS or OS/390 system console to verify that the BBOARS2 server is running.
13. Select HODConfig Servlet, click the right mouse button, and select Activate. Click Yes. Be aware that this step can take some time. Wait for a message that the conversation has been activated.

Installing and running the configuration servlet from the plug-in

To install and run the configuration servlet from the plug-in, add the following to the /*config_dir*/was.conf file (where *config_dir* is the directory where the configuration file is located). Optionally, you can change the default values of the ConfigServerPort, ShowStats and Trace parameters.

```
# ================================================================== #
#
#   The following defines the HOD Configuration Servlet
#
# ================================================================== #
deployedwebapp.HOD.host=default_host
deployedwebapp.HOD.rooturi=/HODConfig
deployedwebapp.HOD.classpath=/usr/lpp/HOD/hostondemand/HOD
     :/usr/lpp/HOD/hostondemand/lib/cfgsrvlt.jar
     :/usr/lpp/HOD/hostondemand/HOD/com/ibm/eNetwork/HODUtil/services/remote
     :/usr/lpp/HOD/hostondemand/HOD/com/ibm/eNetwork/HOD
deployedwebapp.HOD.documentroot=/usr/lpp/HOD/hostondemand/lib
deployedwebapp.HOD.autoreloadinterval=100000
webapp.HOD.jspmapping=*.jsp
webapp.HOD.jspmapping=*.jhtml
webapp.HOD.filemapping=/
webapp.HOD.jsplevel=1.1
webapp.HOD.servlet.HODConfigServlet.code
      =com.ibm.eNetwork.HODUtil.services.remote.HODCfgServlet
webapp.HOD.servlet.HODConfigServlet.servletmapping=/HODConfig
webapp.HOD.servlet.HODConfigServlet.initargs=ConfigServerPort=8999,
       ShowStats=true,Trace=false
webapp.HOD.servlet.HODConfigServlet.autostart=true
############################################################################
```

The three lines following the `deployedwebapp.HOD.classpath` parameter, the line following the `webapp.HOD.servlet.HODConfigServlet.code` parameter, and the line following the `webapp.HOD.servlet.HODConfigServlet.initargs` parameter must be on the same line as the parameter in the actual was.conf file. To improve performance, set the Trace parameter to false.

If you changed the default configuration server port

If you changed the default value of the ConfigServerPort parameter while installing the configuration servlet in the plug-in or the Web container, you need to update the port number in the NSMprop and config.properties.ascii files.

- Add the following line to the /usr/lpp/HOD/hostondemand/private/NSMprop file:

  ```
  CONFIGSERVER_PARMS = %INSTALL_PATH% portnumber
  ```

  where *portnumber* is the new configuration servlet port.
- On a machine that supports ASCII, create a file called config.properties (if it is not already present) and add the following line:

  ```
  ConfigServerPort=portnumber
  ```

  Upload the config.properties file in binary format to the Host On-Demand publish directory on the zSeries system and save it as /usr/lpp/HOD/hostondemand/HOD/config.properties.ascii.

Enable clients to use configuration servlet

You can enable all clients to use the configuration servlet, or you can limit access to specific clients.

- To enable access for all clients, do the following:
  1. On a machine that supports ASCII, create a file called config.properties (if it is not already present) and add the following line:

     ```
     ConfigServerURL=http://server_name/HODConfig/HODConfig/hod
     ```

     where *server_name* is the name of the Host On-Demand server.
  2. Upload the config.properties file in binary format to the Host On-Demand publish directory on the zSeries system and save it as /usr/lpp/HOD/hostondemand/HOD/config.properties.ascii.
- To enable access only for specific clients, do the following:
  1. If it is not already installed, download and install the Deployment Wizard. See “Installing the Deployment Wizard” on page 61 for instructions.
  2. In the HTML model, use the Deployment Wizard to create HTML files and enable the configuration servlet. Set the following parameters in the Additional Parameters window:

     Name ConfigServerURL

     Value /HODConfig/HODConfig/hod

     In the configuration server or combined models, click Server Connection Options on the Additional Options window.
  3. Save the files generated from the Deployment Wizard as a Zip file.
  4. Use FTP to transfer the Zip file to the zSeries system.
  5. Use the DWunzip tool to install the HTML files on the zSeries system. See the online help topic Using DWunzip for more information on how to use this tool.

Verify that the configuration servlet is enabled

Finally, you need to verify that the configuration servlet has been enabled. Do the following:

1. Restart the HTTP server and the Host On-Demand Service Manager.
2. Bring up the HODMain.html file (if you enabled all clients to use configuration servlet) or your own custom Host On-Demand HTML file.
3. Verify that the configuration servlet is enabled by doing one or both of the following:
   - If you set the ShowStats parameter to True when you were installing the cfgservlet.ear file (as described in “Install the configuration servlet” on page 108), you can invoke the ShowStats function to test whether the servlet is running. Specify the following URL in your Web browser:

     ```
     http://server_name/servlet_location/HodConfig/info
     ```

     where *server_name* is the name of the zSeries server and *servlet_location* is the directory in which the configuration servlet is installed (in this example, HODConfig).

     If the configuration servlet is running, the browser window displays statistics gathered from the configuration servlet. The page shows the configuration servlet start time, address, ConfigServerPort, and other information about the servlet. To verify whether the servlet is running, check to see if any POST requests have been processed, if any buffers have been created, and if data has been sent to and received by the Service Manager. Sample statistics from an active configuration servlet are shown in the following excerpt from the statistics HTML file:

```
Servlet Statistics

   Server Information = WebSphere Application Server for OS/390/4.1
   Servlet ID = 0
   152 POST request have been processed. The largest request
      contained 10640 bytes of data.
   The buffer pool currently contains 1 entries.
   A total of 9 buffers have been created.
   A total of 98344 bytes have been transfered to the Service Manager.
   A total of 100140 bytes have been received from the Service Manager.
```

- If you set the Trace parameter to True when you were installing the cfgservlet.ear file (as described in "Install the configuration servlet" on page 108), you can invoke the Trace function to test whether the servlet is running. Specify the following URL in your Web browser:

  ```
  http://server_name/servlet_location/HodConfig/trace
  ```

  where *server_name* is the name of the zSeries server and *servlet_location*.

  If the configuration servlet is running, the browser window displays trace information from the configuration servlet. This sample trace statement for a doPost request indicates that the servlet is active and is successfully handling requests:

  ```
  Fri Mar 01 13:41:07 EST 2002 (98) Called doPost(/hod)
           [93]: 9.37.3.90 <===> mvs059.raleigh.ibm.com:80 user=null[null]
  doPost [93]: got xfer from Pool = null
  doPost [93]: null xfer, creating new one ...
  doPost [93]: done with create!
  doPost [93]: calling doTransfer ...
  doTransfer [93]: transfering data to SM ...
  Fri Mar 01 13:41:07 EST 2002 (217) [93] POST xfer Client ==> SM 258 bytes.
  Fri Mar 01 13:41:07 EST 2002 (596) [93] POST xfer Client <== SM 285 bytes.
  doPost [93]: done with transfer!
  Fri Mar 01 13:41:07 EST 2002 (634) [93] POST - returning
  ```

Setting up separate read/write private and publish directories

Set up a separate HFS for the Host On-Demand private directory

When Host On-Demand is installed, files in the /usr/lpp/HOD/hostondemand/private directory are updated in an execution environment, not just by maintenance (PTF) releases. Because this directory is now updated during the Host On-Demand software's execution, it is recommended that you mount a separate (non-service) HFS. You can do this in one of the following ways:

- MOUNT the separate HFS on the current private directory location, /usr/lpp/HOD/hostondemand/private.
- Create a symbolic link to the private directory location as follows:
  1. Do a TSO MKDIR to create a different mount point, such as /etc/HOD/private.
  2. Rename, or back up and delete, your original private directory.

3. Create a symbolic link from the expected location, /usr/lpp/HOD/hostondemand/private, to point to the real location, /etc/HOD/private. Use the following link command:

   ```
   ln -s /etc/HOD/private /usr/lpp/HOD/hostondemand/private
   ```

Customers running in a sysplex environment using SHARED HFS support can install the Host On-Demand SMP/E managed code in the VERSION HFS, which must be mounted with READ ONLY privileges in a SHARED HFS environment. Make the /private directory a system-specific HFS mounted with READ WRITE privileges, with a symbolic link pointing to the /usr/lpp/HOD/hostondemand/private directory.

If you are using LDAP and native authentication, manually copy the HODrapd and /keys directory to the system-specific /private directory.

When the system-specific /private directory is mounted, it overlays but does not destroy the master /private directory. When maintenance releases are applied, use the master /private directory. If these files were changed, copy them to the system-specific /private directory.

Set up a User publish directory separate from the Host On-Demand publish directory

Under Host On-Demand 7, files that are generated from the Deployment Wizard can be placed in a user-defined directory that is separate from the Host On-Demand publish directory. This makes it easier to apply future Host On-Demand upgrades. It also simplifies installing and maintaining Host On-Demand on OS/390 systems where the SMP/E installed libraries must not contain user modifications (the file systems are mounted read-only). This solution keeps the Host On-Demand publish directory read only and provides a separate writeable location for deploying Deployment Wizard files.

For instructions on deploying Deployment Wizard files in a directory separate from the Host On-Demand publish directory and for information on other user-modified files that can be placed outside the publish directory, see “Backing up files and directories” on page 63.

Chapter 16. Configuring Host On-Demand on iSeries

After you install Host On-Demand on the iSeries platform, configure the software as follows:

- To set up the Service Manager, follow the instructions in “Configuring, starting, and stopping the Host On-Demand Service Manager on iSeries”.
- To use the Deployment Wizard with an iSeries system, follow the instructions in “Using the Deployment Wizard with iSeries” on page 116.
- To configure security, follow the instructions in “Configuring iSeries servers for secure connection” on page 117.

Configuring, starting, and stopping the Host On-Demand Service Manager on iSeries

A menu is provided for starting and stopping the Host On-Demand Service Manager. To access the menu, type the following on the OS/400 command line:

```
GO HOD
```

The following commands can be used from the menu or the OS/400 command line.

Configure (CFGHODSVM)

To configure the Service Manager, choose option 1. You need *JOBCTL and *ALLOBJ authority to use this option. You can configure the following information:

1. Whether to autostart the server when the subsystem starts
2. Adjustment of Java attributes
3. The user ID that the server job uses
4. The subsystem that the server job uses
5. The job description that the server job uses
6. The pre-start class/job priority that the server job uses

There are multiple screens. You may need to page down to see the next screen.

Start (STRHODSVM)

To start the Host On-Demand Service Manager, choose option 2. You need *JOBCTL authority to use this option.

The Service Manager can be automatically started each time that the associated subsystem starts. One way to do this is to add the STRHODSVM command to the system startup program.

To determine whether the Service Manager is running, use the following command:

```
WRKJOB QHODSVM
```

Stop (ENDHODSVM)

To stop the Service Manager, choose option 3. You need *JOBCTL authority to use this option.

Work with HOD Server status

Use this option to view the current status of the Host On-Demand Service Manager.

Certificate Management (WRKHODKYR)

Use this option to work with SSL certificates in one of the Host On-Demand keyrings. Refer to Chapter 5, "Planning for security" on page 27 for general information on SSL related sessions.

Start Information Bundler (STRHODIB)

In the event that you need to contact the IBM Support Center for assistance, use this menu option to gather information about your Host On-Demand configuration.

Create HOD Printer Definition Table (CRTHODPDT)

Use this menu option to create a custom printer definition table for Host On-Demand 3270 printer sessions. A custom printer definition may be necessary if you have a special paper form or if the printer is not supported. Refer to Section 16.5 in the Host Access Client Package Redbook (SG24-6182-00) for additional information.

Start Organizer (STRPCO)

Use this menu option to start the Client Access Organizer for the workstation.

Start a PC Command (STRPCCMD)

Use this menu option to run a command on your PC. You will need to start the Client Access Organizer for the workstation before using this menu option.

Using the Deployment Wizard with iSeries

To use the Deployment Wizard to deploy screens to an iSeries-based Host On-Demand server, do the following:

1. From a Windows workstation, map a network drive to `/qibm` directory on the iSeries system that will be the Host On-Demand server. For additional information, refer to

   `http://publib.boulder.ibm.com/html/`

   `as400/v5r1/ic2924/info/rzahl/rzahlusergoal.htm`

   .
2. Insert the Host On-Demand for Windows CD in the drive. See "Installing the Deployment Wizard" on page 61.
3. A menu will automatically be launched. One of the options is to use the Deployment Wizard. You may run this without having to install the entire Host On-Demand server.
4. Design the custom features and selections.
5. Save the customized HTML file to the mapped network drive (for example, y:\ProdData\hostondemand\hod\myweb).
6. Using a browser, test out the file (for example, http://iSeries.name.com/hod/myweb.html).

Configuring iSeries servers for secure connection

The iSeries servers can be configured to use certificates from a public signing agency or from a private certificate management system, like the AS/400 Digital Certificate Manager. Before you enable SSL, decide which type of certificate to use. See *Deciding where to obtain your digital certificates* on the iSeries Web site (`http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzain/rzainoverview.htm`)

.

You must have the following programs installed to use SSL with iSeries:

- Digital Certificate Manager (DCM), option 34 of OS/400
- TCP/IP Connectivity Utilities for AS/400
- IBM HTTP Server for AS/400
- One of the IBM Cryptographic Access Provider products: 40-bit, 56-bit, or 128-bit. The bit size for these products indicates the varying sizes of the digital keys that they employ. A higher bit size results in a more secure connection. Some of these products are not available in all areas due to government export regulations.

Configuring a Telnet server for secure connection

The following table describes the steps to enable Telnet with SSL. You will need to repeat this step for each iSeries system that you wish to use secure connections with.

OS/400 level	Web page (click on the link for more information)
V5R1 and V5R2	*Secure Telnet* on the iSeries Web site (`http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/index.htm?info/rzain/rzainrzaintelntpi.htm`) . Perform Step 1 only. Client authentication is discussed in "Client authentication" on page 118.
V4R4 and V4R5	*Telnet server and SSL* on the AS/400 Web site (`http://publib.boulder.ibm.com/pubs/html/as400/v4r5/ic2924/info/RZAIWSSLTEL.HTM#HDRRZAIWSSLTEL`)
V4R2 and V4R3	*Telnet SSL Proxy Server* on the AS/400 Web site (`http://www.as400.ibm.com/tstudio/tech_ref/tcp/sslproxy/index.htm`)

Configuring the Host On-Demand CustomizedCAs keyring

If you are using self-signed certificates or certificates from a signing agency that is not in the well-known list, complete the following steps to configure a CustomizedCAs keyring:

1. Type the following command: `GO HOD`.
2. Choose option 5 (Certificate Management).
3. Enter `*CONNECT` for the option and `*CUSTOM` for the name of the keyring, then press the Enter key.
4. Type the TCP/IP name and port for the target server in the following format: *`server.name`*`:`*`port`*

where *server.name* is the TCP/IP name of the target server (for example, my400.myco.com) and *port* is the port for the target server (for example, 992).

This command can take a few minutes to complete. If you are prompted for a password, press the Enter key. If this is the first certificate, a new CustomizedCAs object is created.

5. Select the certificate number that corresponds to the Certificate Authority (CA) that you want to add to the keyring. Be sure to add the CA certificate and not the site certificate. If the port is not responding, refer to “Configuring iSeries servers for secure connection” on page 117.
6. Repeat steps 3-5 for each target server.

To view the contents of the CustomizedCAs keyring, do the following:

1. Type the following command: `GO HOD`.
2. Choose option 5 (Certificate Management).
3. Type `*VIEW` for the option and `*CUSTOM` for the name of the keyring, then press the Enter key.

If you have multiple iSeries machines and would like to create a single certificate that all the machines can use, consider cross certification. Refer to iSeries Wired Security: Protecting Data over the Network, OS/400 Version 5 Release 1DCM and Cryptographic Enhancements (SG24-6168) for additional information about cross certification.

Client authentication

For additional security, consider SSL with client authentication to tightly control who can Telnet to your system over the Internet. For example, you can configure the Telnet server to only allow authentication if the client certificate was issued by your iSeries (through Digital Certificate Manager).

The client certificates have a limited validity period (for example, 90 days). When the certificate expires, the user must perform the Client Certificate Download process in order to continue. This process requires a valid iSeries user ID and password.

Not all Telnet client software is capable of client authentication. When enabled, all SSL-enabled Telnet connections to the iSeries require a user certificate.

OS/400 level	Detailed instructions (click on the link for more information)
V5R1 and V5R2	*Secure Telnet* on the iSeries Web site (`http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/index.htm?info/rzain/rzainrzaintelntpi.htm`)
V4R4 and V4R5	*Telnet Server; SSL Client Authentication* on the TCP/IP for OS/400 Web site (`http://www.ibm.com/servers/eserver/iseries/tcpip/telnet/ssl.htm`)

Configuring the Host On-Demand OS/400 proxy for secure connections

The OS/400 proxy can be configured to encrypt file transfer and Database On-Demand connections. To do this, the following additional software must be installed on each target iSeries:

- IBM Cryptographic Access Provider
- IBM Client Encryption
- Host Servers
- Digital Certificate Manager

Set up SSL user authorizations

You need to control authorization of the users to the files. To help you to meet the SSL legal responsibilities, you must change the authority of the directory that contains the SSL files to control user access to the files. In order to change the authority, do the following:

1. Enter the command `wrklnk '/QIBM/ProdData/HTTP/Public/jt400/*'`
2. Select option 9 in the directory (SSL40, SSL56, or SSL128).
   a. Ensure *PUBLIC has *EXCLUDE authority.
   b. Give users who need access to the SSL files *RX authority to the directory. You can authorize individual users or groups of users. Remember that users with *ALLOBJ special authority cannot be denied access to the SSL files.

Assign certificates to applications

1. From a web browser, access http://*server.name*:2001 (where *server.name* is the TCP/IP host name of your iSeries system). If you are unable to connect, start the HTTP server with the following OS/400 command:
   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```
2. Enter the OS/400 user profile and password (when prompted). You must have *ALLOBJ authority to complete the configuration activities below.
3. Click on **Digital Certificate Manager**.
4. Click on **System Certificates**.
5. Click **Work with Secure Applications**.
6. Click **QIBM_OS400_QZBS_SVR_CENTRAL**, then click **Work with System Certificate**.
7. Verify that the *DFTSVR certificate is selected and click **Assign New Certificate**.
8. Repeat steps 7 and 8 for the following applications:
   - QIBM_OS400_QZBS_SVR_DATABASE
   - QIBM_OS400_QZBS_SVR_DTAQ
   - QIBM_OS400_QZBS_SVR_NETPRT
   - QIBM_OS400_QZBS_SVR_RMTCMD
   - QIBM_OS400_QZBS_SVR_SIGNON
   - QIBM_OS400_QZBS_SVR_FILE
   - QIBM_OS400_QRW_SVR_DDM_DRDA

Repeat the above steps for each target iSeries server.

Configure the OS/400 proxy keyring

If any of the target connections is using self-signed certificates or certificates from a signing agency that is not on the well-known list, do the following:

1. Type the following command: `GO HOD`.
2. Choose option 5 (Certificate Management).
3. Enter `*CONNECT` for the option and `*PROXY` for the name of the keyring, then press the Enter key.
4. Type the TCP/IP name and port for the target server in the following format:

   ```
   server.name:port
   ```

   where *server.name* is the TCP/IP name of the target server (for example, my400.myco.com) and *port* is the port for the sign-on server (for example, 9476).

   This command can take a few minutes to complete. If you are prompted for a password, press the Enter key. If this is the first certificate, a new KeyRing.class object is created.
5. Select the certificate number that corresponds to the Certificate Authority (CA) that you want to add to the keyring.
6. Repeat steps 3-5 for each target server.

Secure Web serving

The Host On-Demand server uses the Web server to download program objects to the browser. This information can be encrypted, but with a considerable performance impact. Refer to the redbook AS/400 HTTP Server Performance and Capacity Planning (SG24-5645) for more information.

The default port for secure web serving is 443. If that port is not enabled, port 80 is used. To enable secure web serving, perform the following steps:

1. From a Web browser, enter: `http://<server.name>:2001` (where <server.name> is the TCP/IP host name of your iSeries). If you are unable to connect, start the HTTP server with the following OS/400 command:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```
2. Enter the OS/400 user profile and password (when prompted). You must have *ALLOBJ and *SECADM authorities to complete the remaining configuration activities.
3. Click IBM HTTP Server for AS/400.
4. Click Configuration and Administration.
5. Click Configurations.
6. Select the CONFIG configuration from the list.
7. Click Security Configuration.
8. For the Allow HTTP connections and Allow SSL connections selections:
   - Port number (443)
   - Select SSL Client authentication None.
   - Select Apply.
9. Click AS/400 Tasks button on the lower left side of the screen.
10. Click Digital Certificate Manager.
11. Click System Certificates.
12. Click Work with Secure Applications.
13. Click QIBM_HTTP_SERVER_CONFIG; then click Work with System Certificate.
14. Click Assign New Certificate.

15. End the administration HTTP server instance with the following OS/400 command:

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

16. Wait 10 seconds for the HTTP instance to shut down.
17. Start the administration HTTP server instance with the following OS/400 command:

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

18. From a Web browser, enter `https://`*`server.name`*`/hod/hodmain.html` (where *server.name* is the TCP/IP host name of your iSeries).

For more information on a wide variety of iSeries topics, see www.redbooks.ibm.com/tstudio.

Chapter 17. Deploying Host On-Demand With WebSphere Portal

As an alternative to accessing Host On-Demand through an HTML file, users can access it through Portal Server, which is a component of WebSphere Portal. Portal Server provides a framework for plugging content extensions known as *portlets* into a Web site. Portlets are applications that run within Portal Server. They organize content from different sources (such as Web sites, e-mail, and business applications) and display it on a single HTML file in a browser window. The HTML files that are used to launch Host On-Demand sessions can be deployed as portlets, enabling users to access Host On-Demand through the portal interface. If you are planning to use Host On-Demand and Websphere Portal Server in conjunction with a firewall, refer to “Using Host On-Demand with a firewall” on page 33.

Both Host On-Demand and Portal Server must be installed in order to run a Host On-Demand portlet.

How Host On-Demand works with Portal Server

Figure 8 shows how Host On-Demand works with Portal Server.

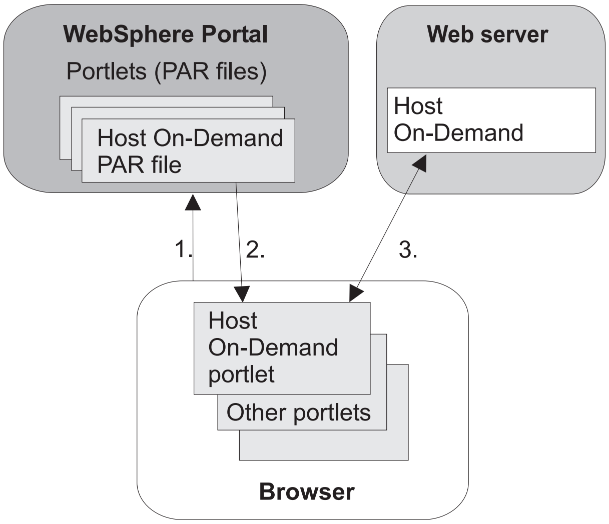

Figure 8. How Host On-Demand works with Portal Server

1. A user logs into the portal through a browser and is authenticated by a user ID and password.
2. The user’s customized set of portlets is downloaded to the user’s machine and is displayed in the browser.
3. If the user has configured a Host On-Demand portlet, Host On-Demand starts. This gives the user full Host On-Demand functionality within the portlet window, including being able to start sessions and perform other Host On-Demand tasks.

Using Host On-Demand clients with Portal Server

To use Host On-Demand with Portal Server, you need a Host On-Demand portlet. You can quickly and easily create your own custom portlets using the Deployment Wizard. See the Deployment Wizard online help for details about creating portlets. You can also download sample Host On-Demand portlets either from the Host On-Demand Service Key site at `http://www6.software.ibm.com/aim/home.html` on the Host On-Demand CSD page under Tools and Utilities, or from the Portal Server portlet catalog at `http://www7b.software.ibm.com/webapp/portlets/portletemarketplace`.

After you create a custom portlet or obtain a sample one, you can import it directly into Portal Server just like any other portlet. See the Websphere Portal InfoCenter Web site at `http://www.ibm.com/software/webservers/portal/library` for more details.

Limitations on accessing Host On-Demand through a portlet

The Portal supports full Host On-Demand functionality with the following limitations:

- Multiple Host On-Demand portlets cannot be run on the same Portal Server page.
- If the portlet uses caching for Host On-Demand (as configured in the Deployment Wizard), each machine used to access the portlet caches the Host On-Demand client.
- If the portlet configuration allows users to make updates that are saved on their local machines (as specified in the Deployment Wizard), an update made by a user from one machine is not available if that user accesses the portlet from a different machine.
- Host On-Demand bookmarking does not work in the portal environment.
- If the applet size is not configured in the Deployment Wizard, it will default to fixed size, medium.

Special considerations when using a Host On-Demand portlet

When using Host On-Demand with Portal Server, you may want to consider the following issues:

- **Setting the Host On-Demand applet size for the client.** If you would like an applet size that is different from the available options in the Deployment Wizard, you can modify the portlet to specify pixel width and height. To do this, you will first need to extract the portlet and locate the file called WpsHODFinal.jsp. (See the section below titled ″Extending the Host On-Demand Portlets″ for details on extracting and repackaging the portlet.) In this file, locate the two lines beginning with var hod_AppHgt and var hod_AppWid. These are JavaScript variables defining the applet dimensions. Edit the quantities assigned to each of these variables with the dimensions you desire. Save the file, repackage the portlet, and install the portlet in your portal.
- **Host On-Demand sessions when the user logs out of Portal Server.** Host On-Demand runs as an applet on the user's machine and therefore does not know when the user logs out of Portal Server. If the session is running in a separate window (default), the Host On-Demand session will continue until the user either closes the session or closes the browser. If the Host On-Demand session is running embedded in the Portal Server window and the user logs out of Portal Server, the session may appear to have ended, although the connection

may remain until the browser window is closed. We strongly recommend that users close their browser window at the time they log out of Portal Server. In addition, you may wish to configure a session inactivity timeout for your sessions.

- **Session inactivity timeout**. By default, Host On-Demand does not force a timeout on session connections. However, when running a portlet, it may be beneficial to timeout inactive sessions to reduce consumption of resources. The inactivity timeout can be set for most emulator types, including 3270 display and printer sessions, 5250 display and printer sessions, and VT. You can enable and set the timeout parameter Session Inactivity Timeout in minutes for both display and printer sessions from the `Advanced Tab` in the session properties panel.
- **Installing Websphere Portal and Host On-Demand on different servers**. If you install Websphere Portal and Host On-Demand on different servers, certain browsers, such as Netscape 6, may give you a security violation when accessing the Host On-Demand portlet. The problem occurs because some aspects of Host On-Demand functionality rely heavily on the interaction between Java (from the Host On-Demand server) and JavaScript (from Websphere Portal), and some browsers will not allow the interaction simply because they come from different servers. One solution is to use proxying to make it appear to the browser that Websphere Portal and Host On-Demand are on the same server. Below is an example of the steps you would need to follow to set up proxying on the Apache/IBM HTTP server:
  1. Configure your Host On-Demand portlet's "HOD Server URL" (hodCodeBase) to point to the host on which WebSphere Portal resides, with the context root of /hod/ (for example, http://portal.company.com/hod).
  2. Uncomment the line (remove the #) in httpd.conf beginning with LoadModule proxy_module.
  3. Add a ProxyPass rule to httpd.conf to convert the HOD Server URL request into a request for the actual Host On-Demand server (for example, ProxyPass /hod/ http://hod.company.com/hod/).
  4. Restart the Web server.

  Now, the client's browser will request Host On-Demand files from the same host as the portal, but these requests will be internally rerouted by the Web server to the actual location of your Host On-Demand install.
- **Caching vs. no caching**. The default setting in the Deployment Wizard is to cache Host On-Demand on each user's machine. Many customers like this option with Host On-Demand because it effectively installs all necessary code on the user's machine and does not require network loads each time the user accesses the HTML file or portlet. However the caching behavior may not be familiar to many Portal Server users, and you may elect to reject the caching option.
- **Choosing the Deployment Wizard model**. The model you choose for your portlet (Configuration-Server, HTML, or Combined) will reflect where your sessions are configured and will determine how user changes are stored. Although Host On-Demand treats portlets the same as HTML files, consider the following characteristics as you decide how to configure your portlet:
  - HTML model: This model has no dependency on the Host On-Demand Configuration Server. If users are allowed to make updates, their changes will be stored on their local machines. These user changes will not be available if the user roams to a different machine.

  - Configuration-Server model: This model requires user access to the Host On-Demand Configuration Server. It allows your users to roam from one machine to another and still see any session modifications they may have made.
  - Combined model: This model requires users to have access to the Host On-Demand Configuration Server in order to obtain the initial session configurations. Any user updates will be saved to the user's local machine and will not be available on a different machine if the user roams.
- **Defining embedded sessions**. By default, Host On-Demand sessions are configured to launch in a separate browser window. You can choose to have the sessions launch in the same window by selecting the Advanced tab in Session Properties and setting Start in a Separate Window to No.
- **Starting the session automatically**. By default, Host On-Demand sessions will not start until the user selects the icon to start. If you wish to have the session start automatically, select the Advanced tab in Session Properties and set Start Automatically to Yes.
- **Setting the portlet's access control in Portal Server**. The Host On-Demand portlet does not have any fields that a user can edit using the portlet interface. Therefore, when you import the portlet into Portal Server, you should set the access control to be viewable, but not editable.

Extending the Host On-Demand portlets

Under certain circumstances, you may wish to modify the appearance or functionality of your Host On-Demand portlets. Here are some tips and guidelines to help you extend your portlets:

- Portlet template files are located in the portal subdirectory of your Host On-Demand publish directory (or in your Deployment Wizard installation directory, if you installed it separately). Modifying these templates will affect all portlets that are generated subsequently, so be sure to back up these files if you are going to modify them. Template files include those for the JSPs that are used to display the Host On-Demand applet and those for the XML descriptors that are used to deploy the portlets to WebSphere Portal.
- Each portlet is an archive that can easily be extracted and re-archived using a zip utility or the jar utility packaged with a JRE. Extract the portlet to a temporary directory, preserving directory names. You can then modify the appropriate files, and re-archive the portlet from the top level of the temporary directory.
- XML descriptors are located in the top-level directory of your portlet. JSP files are located in the /PORTLET-INF/hod/html directory for WebSphere Portal Family 2.1, and in the /WEB-INF/hod/html directory for WebSphere Portal 4.1.
- You may wish to add a custom Help file to your portlet. To do this, you must indicate in your portlet.xml file that you support the *help* markup mode. Add a file named WpsHODHelp.jsp (case-sensitive) containing your help information and HTML formatter to your JSP directory in your portlet.
- You may wish to develop a custom portlet that dynamically modifies session properties. Some useful data you may want to access would be the user name of the portal user, or the IP address of the client requesting the page. Consult the portlet APIs on how to access this data. You can use the HTML override syntax described in Chapter 14, "Modifying session properties dynamically" on page 95 to then insert data derived from this information into your set of applet parameters.

- Consult the WebSphere Portal InfoCenter installed with WebSphere Portal for detailed information regarding portlet development and APIs.

Chapter 18. Configuring Host On-Demand Server to use LDAP

The Host On-Demand Server is used to manage configuration data for the configuration server-based and combined models. For the default operational mode of the Host On-Demand Server, this data is saved in a non-shared private data store. Some enterprise customers need to manage their configuration information between multiple Host On-Demand servers. If these customers use the non-shared private data store, then their administrators must manage the data for each Host On-Demand Server separately. A Lightweight Directory Access Protocol (LDAP) server directory provides the ability to share user and group configuration information configuration information over different instances of the Host On-Demand configuration server.

Using an LDAP directory server to manage and share your definitions across multiple Host On-Demand servers is an option that must be carefully planned and executed. Migration from the private data store, in particular, has implications on the configuration data. LDAP enables the customer to manage the configuration information by arranging users into a hierarchical tree of groups. If existing users are members of more than one group, then some information will be lost. Note that the configuration data in the private data store is not changed when a migration to LDAP occurs. Refer to implications of migrating to LDAP in the Host On-Demand online help for more detailed information.

Setting up LDAP support

1. Decide which LDAP Directory server you are going to use and, if necessary, install it. See “Supported LDAP servers” on page 16 for a list of the LDAP servers supported on your Host On-Demand server platform. .
2. If you are running a version of LDAP that does not support the schema for Host On-Demand , install the Host On-Demand schema extension files as described in “Installing the schema extensions” on page 130. (The schema extension files are not required for IBM LDAP Version 3.x.)
3. Ask your LDAP administrator for a suffix which Host On-Demand will use to store configuration information. Make a note of the distinguished name (DN) of this suffix; you will need this information to complete the LDAP setup.
4. Ask your LDAP administrator for an administrator DN and password for Host On-Demand; these will be used to authenticate to the LDAP server. The administrator DN must have create, modify and delete privileges for the suffix mentioned in the previous step. Make a note of the DN and password; you will need this information to complete the LDAP setup.
5. Enable LDAP on the Directory tab in the administration window. Also, optionally, migrate the private data store configuration information to the LDAP directory server. For more information, refer to Chapter 18, “Configuring Host On-Demand Server to use LDAP”.

Users and groups that are already defined in LDAP for other purposes are not used by Host On-Demand. Users and groups for Host On-Demand must be defined separately by either migrating the configuration information from the private data store or by setting up the users and groups in Host On-Demand after enabling LDAP.

Installing the schema extensions

The Host On-Demand extensions to the LDAP directory schema are provided in several files that are located in the LDAP subdirectory of the publish directory (for example, `C:\hostondemand\HOD\ldap)` . These files contain extensions to the LDAP schema and are stored in the standard slapd format. The schema extensions must be in effect before Host On-Demand can store configuration information in an LDAP server. Contact your LDAP administrator to have these schema extensions installed.

Refer to the Program Directory for instructions on installing the schema extensions for the zSeries.

Your LDAP administrator may have already installed these schema extensions for use by another IBM product. If so, skip these steps. If you are using the IBM SecureWay Directory Server Version 3.1.1 or 3.2.1, the schema is pre-installed, so you can skip these steps also.

To install the Host On-Demand schema extensions on a Netscape LDAP Directory server:

1. Copy the following slapd files from the <Host On-Demand publish directory>/ldap directory to the Netscape LDAP config directory on the LDAP server :
   ```
   Netscape.IBM.at
   Netscape.IBM.oc
   ```
2. Stop the LDAP server.
3. Edit the <Netscape LDAP config directory>/`slapd.conf` file and add the following statements:
   ```
   userat "<Netscape LDAP config directory>/Netscape.IBM.at"
   useroc "<Netscape LDAP config directory>/Netscape.IBM.oc"
   ```
4. Restart the LDAP Server.

To install the Host On-Demand schema extensions on an IBM LDAP Directory server:

1. Copy the following slapd files from the Host On-Demand publish directory/ldap directory to the <installation directory>/etc directory on your LDAP server:
   ```
   V2.1.IBM.at
   V2.1.IBM.oc
   ```
2. Stop the LDAP server.
3. Edit the <installation directory>/etc/`slapd.at.conf` file and add the following statement to the end of the file:
   ```
   include /etc/V2.1.IBM.at
   ```
4. Edit the <installation directory>/etc/`slapd.oc.conf` file and add the following statement to the end of the file:
   ```
   include /etc/V2.1.IBM.oc
   ```
5. Restart the LDAP server.

Configuring the Host On-Demand server to use LDAP as a data store

1. Open the Administration window and logon to Host On-Demand.
2. Click Services > Directory Service

3. Click the Use Directory Service (LDAP) box and then enter the LDAP server information.

   Destination Address
   Type the IP address of the LDAP directory. Use either the host name or dotted decimal format. The default is the host name 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`).

   Migrate Configuration to Directory Service
   To migrate users and groups from the private data store to the LDAP directory, click the check box. Migrating to LDAP has significant implications for your group and user configuration information. Refer to LDAP Migration Implications in the online help for more information. You can check this box either when you switch to the directory server, or after you have made the switch.

The Redirector configuration is not migrated to the directory server.

If you have a problem connecting to LDAP and migrating, try to connect to LDAP first. Then, after successfully connecting, try to migrate.

4. Click Apply.

   When you are asked to authenticate with the LDAP directory for the first time, specify a user ID of ″admin″ and a password of ″password″. You can change this password after the first log on. Even though you might have changed your password for the private data store, that ID and password continues to be valid for the private data store only. For the LDAP directory, a separate user ID and password are required. To avoid confusion, you can change your LDAP directory password to be the same as your private data store password.

Changes made on this panel are effective immediately. Once you have switched to the LDAP server, subsequent user-related changes will be made only on the LDAP server, including administrative changes to groups, users, or sessions, and changes such as new passwords, macros, keyboard changes, etc., by either the administrator or a user.

Appendix A. Manually installing SSL security capability on AIX

If you intend to use an AIX server to support secure connections from clients, you must install additional files.

Before installing the AIX server security files over an existing installation, remove all lib*.so files from the hostondemand/bin directory.

If you are running AIX 4.2, you must first upgrade to AIX 4.3, uninstall the previous version of Host On-Demand, and install Host On-Demand 7 using the hod70srv.AIX43.SSL.tar file.

You must also install JDK 1.1.8 or 1.3.

The following steps assume you are using the default server and publish directories. To install the security files:

1. Enter the following commands to unpack the main file:
   ```
   cd /usr/opt/hostondemand
   tar -xf /cdrom/tar/HOD70AIX.tar
   ```
2. The file extracted from HOD70AIX.tar is hod70srv.AIX43.SSL.tar. This file contains security files to be added to the server directory of an AIX 4.3 installation.
3. To add the extra files to the installation, untar the hod70srv.AIX43.SSL.tar file to the server directory. Enter the following commands:
   ```
   cd /usr/opt/server_directory
   rm bin/lib*.so
   tar -xf ./hod70srv.AIX43.SSL.tar
   ```
4. The GSK security library must also be installed. To extract the installp images, enter the following commands:
   ```
   cd /cdrom/tar/
   ```

   From the current directory, type `smit` to start the System Management Interface Tool (SMIT):
   a. From the System Management screen, click Software Installation and Maintenance.
   b. Click Install and Update Software.
   c. Click Install and Update from ALL Available Software.
   d. Type `./` when asked for INPUT device/directory, then click OK.
   e. Click List in the SOFTWARE to install field.
   f. In the list of software to install, highlight the line labeled gskkm, then click OK.
   g. Click OK on the Install and Update From ALL Available Software window.
   h. Click OK to close the confirmation message and install the software.

Before it starts, the Certificate Management program copies the English version of its help files to the hostondemand/bin directory. This is done by the following line in the file hostondemand/bin/CertificateManagement:

```
cp en/HODServerKMHelp.class
```

If you want to have access to the help for a different language, you must change the directory from which the HODServerKMHelp.class file is copied. For example, if you want to use the Spanish help files, change the above line to:

```
cp es/HODServerKMHelp.class
```

Appendix B. Using locally installed clients

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

Operating systems that support the locally installed client

Host On-Demand can be installed as a client on the following operating systems:

- Windows 95
- Windows 98
- Windows Millennium (Me)
- Windows NT 4.0 with SP3 or later
- Windows 2000
- Windows XP (32-bit)

The locally-installed client requires 155 MB of disk space.

Installing the local client

To install the Host On-Demand local client on a Windows NT, Windows 2000, or Windows XP workstation, you must be a member of the Administrators group.

1. Insert the CD and run `setup.exe lc` from the `\win32` directory of the CD.
2. Click Install.
3. Choose a Typical or Custom installation.
   - Typical installs the Host On-Demand Java applets and the information library in English and the native language of your workstation.
   - Custom allows you to choose components to install: Host On-Demand Java applets, the information library and the Host Access Class Library. In addition to English, you can also select any of the other supported languages.
4. Proceed through the rest of the windows.
5. If you have not already done so, read the Readme available in the last window.

At the end of installation, the Host On-Demand Service Manager is configured and started automatically. On Windows NT, Windows 2000, and Windows XP, the Service Manager is installed as a Service; on Windows 95, Windows 98, and Windows Millennium (Me) it is added to the Start menu.

Starting the local client

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

Removing the local client

1. Stop the Host On-Demand Service Manager:
   a. Press `Ctrl+Alt+Del` once to open the Close Program window.
   b. Highlight the JRE task, then click End Task.
2. Use Add/Remove Programs from Control Panel. If InstallShield does not remove the `hostondemand` directory, you must remove it manually.

Appendix C. Using the IKEYCMD command-line interface

IKEYCMD is a command-line tool, in addition to the Host On-Demand Certificate Management Utility, that can be used to manage keys, certificates, and certificate requests. It is functionally similar to Certificate Management and is meant to be run from the command line without a graphical interface. It can be called from native shell scripts and programs to be used when applications prefer to add custom interfaces to certificate and key management tasks. It can create key database files for all of the types that the Certificate Management utility currently supports. It can create certificate requests, import CA-signed certificates and manage self-signed certificates. It is Java-based and is available only on Windows and AIX platforms.

Use IKEYCMD for configuration tasks related to public-private key creation and management. You cannot use IKEYCMD for configuration options that update the server configuration file, httpd.conf. For options that update the server configuration file, you must use the IBM Administration Server.

Environment set up for IKEYCMD command-line interface

Set up the environment variables to use the IKEYCMD command-line interface as follows:

For Windows platforms, do the following:

- Using the user interface or by modifying autoexec.bat on a command window, set/modify the PATH variable to include the location of the Java executable files:
  ```
  set PATH=c\hostondemand\bin;%PATH%;
  ```
- Using the user interface or by modifying autoexec.bat on a command window, set/modify the CLASSPATH environment variable as follows:
  ```
  set CLASSPATH=c\Program Files\ibm\gsk5\classes\cfwk.zip;C:\
  Program Files\ibm\gsk5\classes\gsk5cls.jar;%CLASSPATH%;
  ```

For AIX platforms, do the following:

- Set your PATH to where your Java or JRE executable resides:
  ```
  EXPORT PATH=/opt/IBMJava/bin:$PATH
  ```
- Set the following CLASSPATH environment variable:
  ```
  EXPORT CLASSPATH=/usr/local/ibm/gsk/classes/cfwk.zip:/
  usr/local/ ibm/gsk/classes/gsk4cls.jar:$CLASSPATH
  ```

Once completed, IKEYCMD should run from any directory. To run an IKEYCMD command, use the following syntax:

```
java com.ibm.gsk.ikeyman.ikeycmd <command>
```

IKEYCMD command-line syntax

The syntax of the Java CLI is

```
java [-Dikeycmd.properties=<properties_file>],
com.ibm.gsk.ikeyman.ikeycmd <object> <action> [options]
```

where

- -Dikeycmd.properties specifies the name of an optional properties file to use for this Java invocation. A default properties file, ikminit_hod.properties, is provided as a sample file that contains the default settings for Host On-Demand.
- Object is one of the following:
  - -keydb: actions taken on the key database (either a CMS key database file or SSLight class)
  - -cert: actions taken on a certificate
  - -certreq: actions taken on a certificate request
  - -help: display help for the IKEYCMD invocations
  - -version: display version information for IKEYCMD

Action is the specific action to be taken on the object, and options are the options, both required and optional, specified for the object and action pair.

The object and action keywords are positional and must be specified in the selected order. However, options are not positional and can be specified in any order, provided that they are specified as an option and operand pair.

IKEYCMD list of tasks for Host On-Demand

IKEYCMD command-line interface tasks required for Host On-Demand are summarized in the following sections of this appendix:

- "Creating a new key database"
- "Listing CAs" on page 140
- "Showing the default key in a key database" on page 145
- "Storing the encrypted database in a stash file" on page 145
- "Creating a new key pair and certificate request" on page 140
- "Storing the server certificate" on page 141
- "Creating a self-signed certificate" on page 142
- "Making server certificates available to clients" on page 143
- "Exporting keys" on page 144
- "Importing keys" on page 144

Creating a new key database

A key database is a file that the server uses to store one or more key pairs and certificates. This is required to enable secure connections between the Host On-Demand server and clients. Before configuring SSL communication, you must create the HODServerKeyDb.kdb key database file in *your_install_directory*\bin for Windows and *your_install_directory*/bin for AIX. This file is not shipped with Host On-Demand, so you must create it after the first install.

For Windows platforms, for example, to create a new key database using the IKEYCMD command-line interface, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -type cms -expire <days> -stash
```

where *your_install_directory* is your Host On-Demand installation directory.

Note the following descriptions:

- <password>: Password is required for each key database operation. Even though a database of the type sslight requires a specified password, the password can be a NULL string (specified as "").
- -type: the HODServerKeyDb.kdb used by the Host On-Demand server is of the type CMS.
- -expire: Days before password expires.
- -stash: Stashes password for key database. Stashing the password is required for the IBM HTTP Server and the Host On-Demand server.

  When the -stash option is specified during the key database creation, the password is stashed in a file with the filename HODServerKeyDb.sth

  Once the HODServerKeyDb.kdb file has been created, it holds all the security information needed by the Host On-Demand server. Any additions or changes are made to the existing HODServerKeyDb.kdb key database file.

Whenever you create or make changes to the HODServerKeyDb.kdb file, you must stop and restart the Host On-Demand Service Manager.

Setting the database password

When you create a new key database, you specify a key database password. This password protects the private key. The private key is the only key that can sign documents or decrypt messages encrypted with the public key. Changing the key database password frequently is a good practice.

Use the following guidelines when specifying the password:

- The password must be from the U.S. English character set.
- The password should be at least six characters and contain at least two nonconsecutive numbers. Make sure the password does not consist of publicly obtainable information about you, such as the initials and birth date for you, your spouse, or children.
- Stash the password.

Keep track of expiration dates for the password. If the password expires, a message is written to the error log. The server will start, but there will not be a secure network connection if the password has expired.

Changing the database password

To change the database password, type:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -changepw
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -new_pw <new_password> -expire <days> -stash
```

where *your_install_directory* is your Host On-Demand installation directory.

Note the following descriptions:

- -new_pw: New key database password; this password must be different than the old password, and this password cannot be a NULL string.
- -expire: Days before password expires.
- -stash: Stashes password for key database. Stashing the password is required for the IBM HTTP Server and the Host On-Demand server.

Listing CAs

To display a list of trusted CAs in the HODServerKeyDb.kdb key database, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -list CA
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password>-type cms
```

where *your_install_directory* is your Host On-Demand installation directory.

By default, HODServerKeyDb.kdb comes with the CA certificates of the following well-known trusted CAs:

- IBM World Registry CA
- Integrion CA Root (from IBM World Registry)
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 4 Public Primary CA
- VeriSign Test CA
- RSA Secure Server CA (from VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

Creating a new key pair and certificate request

To create a public-private key pair and certificate request, do the following:

1. For Windows platforms, for example, enter the following command:

   ```
   java com.ibm.gsk.ikeyman.ikeycmd -certreq -create
   -db your_install_directory\bin\HODServerKeyDb.kdb
   -pw <password> -size <1024 | 512> -dn <distinguished_name>
   -file <filename> -label <label>
   ```

   where *your_install_directory* is your Host On-Demand installation directory.

   Note the following descriptions:

   - -size: key size of 512 or 1024
   - -label: label attached to certificate or certificate request
   - -dn: X.500 distinguished name. This is input as a quoted string of the following format: (Only CN, O, and C are required; CN=common_name, O=organization, OU=organization_unit, L=location, ST=state/province, C=country.)

     ```
     "CN=weblinux.raleigh.ibm.com,O=ibm,OU=IBM HTTP Server,L=RTP,ST=NC,C=US"
     ```
   - -file: name of file where the certificate request will be stored. By default, Host On-Demand uses the name certreq.arm and it should be stored in the \hostondemand\bin directory, where HODServerKeyDb.kdb is located.
2. Verify that the certificate was successfully created.

a. View the contents of the certificate request file you created.

b. Make sure the key database recorded the certificate request:

```
java com.ibm.gsk.ikeyman.ikeycmd -certreq -list
-db <filename> -pw <password>
```

You should see the label listed that you just created.

3. Send the newly created file to a certificate authority.

Storing the server certificate

Receiving a CA-signed certificate

Use this procedure to receive an electronically mailed certificate from a certificate authority (CA), designated as a trusted CA on your server. By default, the following CA certificates are stored in the HODServerKeyDb.kdb key database and marked as trusted CA certificates:

- IBM World Registry CA
- Integrion CA Root (from IBM World Registry)
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 4 Public Primary CA
- VeriSign Test CA
- RSA Secure Server CA (from VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

The Certificate Authority may send more than one certificate. In addition to the certificate for your server, the CA may also send additional Signing certificates or Intermediate CA Certificates. For example, Verisign includes an Intermediate CA Certificate when sending a Global Server ID certificate. Before receiving the server certificate, receive any additional Intermediate CA certificates. Follow the instructions in “Storing a CA certificate” on page 142 to receive Intermediate CA Certificates.

If the CA who issues your CA-signed certificate is not a trusted CA in the key database, you must first store the CA certificate and designate the CA as a trusted CA. Then you can receive your CA-signed certificate into the database. You cannot receive a CA-signed certificate from a CA who is not a trusted CA. For instructions, see “Storing a CA certificate” on page 142

For Windows platforms, for example, to receive the CA-signed certificate into a key database, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -receive -file <filename>
-db your_install_directory\bin\HODServerKeyDb.kdb -pw <password>
-format <ascii | binary> -default_cert <yes | no>
```

where *your_install_directory* is your Host On-Demand installation directory.

Note the following descriptions:

- -format: Certificate Authority might provide CA Certificate in either ASCII or binary format
- -label: Label attached to CA certificate.
- -trust: Indicates whether this CA can be trusted. Use enable options when receiving a CA certificate.
- -file: File containing the CA certificate.

Storing a CA certificate

For Windows platforms, for example, to store a certificate from a CA who is not a trusted CA, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -label <label> -format <ascii | binary>
-trust <enable |disable> -file <file>
```

where *your_install_directory* is your Host On-Demand installation directory.

Note the following descriptions:

- -label: Label attached to certificate or certificate request
- -format: Certificate Authorities might supply a binary ASCII file
- -trust: Indicate whether this CA can be trusted. This should be Yes.

You must stop and restart the Host On-Demand Service Manager after doing this.

Creating a self-signed certificate

It usually takes two to three weeks to get a certificate from a well-known CA. While waiting for an issued certificate, use IKEYCMD to create a self-signed server certificate to enable SSL sessions between clients and the server. Use this procedure if you are acting as your own CA for a private Web network.

For Windows platforms, for example, to create a self-signed certificate, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -size <1024 | 512> -dn <distinguished name>
-label <label> -default_cert <yes or no>
```

where *your_install_directory* is your Host On-Demand installation directory.

Note the following descriptions:

- -size: Key size 512 or 1024
- -label: Enter a descriptive comment used to identify the key and certificate in the database.
- -dn: Enter an X.500 distinguished name. This is input as a quoted string of the following format (Only CN, O, and C are required; CN=common_name, O=organization, OU=organization_unit,L=location, ST=state, province, C=country).

  ```
  "CN=weblinux.raleigh.ibm.com,O=ibm,OU=IBM HTTP Server,L=RTP,ST=NC,C=US"
  ```

- -default_cert: Enter yes, if you want this certificate to be the default certificate in the key database. If not, enter No.

Making server certificates available to clients

All the certificates in the HODServerKeyDb.kdb are available to the Host On-Demand server. However, in some of the configurations, one of these certificates must also be made available to the clients that access the server. In the cases where your server uses a certificate from an unknown CA, the root of that certificate must be made available to the client. If your server uses a self-signed certificate, then a copy of that certificate must be made available to the clients.

For Host On-Demand downloaded and cached clients, this is done by extracting the certificate to a temporary file and creating or updating a file named CustomizedCAs.class, which should be present in the Host On-Demand publish directory. For Windows, the default publish directory is \hostondemand\HOD, and for AIX, the default publish directory is usr/opt/hostondemand/HOD.

To create the CustomizedCAs.class file for downloaded or cached clients, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb
-create -db CustomizedCAs.class -type sslight
```

It will prompt for a password. Simply press Enter, which implies a NULL password. After the CustomizedCAs.class file has been created, you will need to add the server certificate to it.

Adding the root of an unknown CA to CustomizedCAs.class

First, extract the CA's root certificate or a self-signed certificate from the HODServerKeyDb.kdb key database file. To do this, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -extract
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -label <label> -target cert.arm -format ascii
```

where *your_install_directory* is your Host On-Demand installation directory.

Note the following descriptions:

- -label : Label attached to the certificate.
- -pw: password to open HODServerKeyDb.kdb key database file.
- -target : Destination file or database. In this case, it is the name of the Base-64 Armored ASCII format file with a default filename of cert.arm.
- -format: Can be either ASCII or Binary.

Now, add this CA root certificate to the CustomizedCAs.class file. To add a CA root certificate or a self-signed certificate to the list of signers in CustomizedCAs.class, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db CustomizedCAs.class -label <label>
-file cert.arm -format ascii -trust <enable | disable>
```

Note the following descriptions:

- -label: Label for the certificate being added.

- -file: Name of the file where the certificate has been extracted to. In this case, it is the name of the Base-64 Armored ASCII format file with a default filename of cert.arm.
- -format: Can be ASCII or Binary.
- -trust: Decides whether to set as a trusted root. Enable will set the CA root or self-signed certificate as a trusted root. Disable will not set the CA root or self-signed certificate as a trusted root.

Stop and restart the Host On-Demand Service Manager after completing this task.

Exporting keys

To export keys to another key database or to export keys to a PKCS12 file, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -export -db <filename>
-pw <password> -label <label> -type <cms | sslight>
-target <filename> -target_pw <password>
-target_type <cms | sslight | pkcs12> -encryption <strong | weak>
```

Note the following descriptions:

- -label : Label attached to the certificate.
- -target : Destination file or database.
- -target_pw : Password for the target key database.
- -target_type : Type of the database specified by -target operand
- -encryption : Strength of encryption. Default is strong.

Importing keys

To import keys from another key database, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -import -db <filename>
-pw <password> -label <label> -type <cms | sslight> -target
<filename> -target_pw <password> -target_type <cms | sslight>
```

To import keys from a PKCS12 file,enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -import -file <filename>
-pw <password> -type pkcs12 -target <filename>
-target_pw <password> -target_type <cms | sslight>
```

Note the following descriptions:

- -label: Label attached to the certificate.
- -target: Destination database.
- -target_pw: Password for the key database if -target specifies a key database
- -target_type : Type of the database specified by -target operand.

Showing the default key in a key database

For Windows platforms, for example, to display the default key entry, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -getdefault
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password>
```

where *your_install_directory* is your Host On-Demand installation directory.

Storing the encrypted database in a stash file

For a secure network connection, store the encrypted database password in a stash file. For Windows platforms, for example, to store the password while a database is created, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <password> -type cms -expire <days> -stash
```

where *your_install_directory* is your Host On-Demand installation directory.

For Windows platforms, for example, to store the password after a database has been created, enter the following command:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -stashpw
-db your_install_directory\bin\HODServerKeyDb.kdb -pw <password>
```

where *your_install_directory* is your Host On-Demand installation directory.

Using GSK5CMD batch file

A batch file, gsk5cmd, provides the same function of the ″java com.ibm.gsk.ikeyman″ command. For Windows platforms, for example, to store the password after a database has been created, you can also enter following command:

```
gsk5cmd -keydb -stashpw
-db your_install_directory\bin\HODServerKeyDb.kdb -pw <password>
```

where *your_install_directory* is your Host On-Demand installation directory.

IKEYCMD command-line parameter overview

The following table describes each action that can be performed on a specified object.

Object	Action	Description
-keydb	-changepw	Change the password for a key database
	-convert	Convert the key database from one format to another
	-create	Create a key database
	-delete	Delete the key database

	-stashpw	Stash the password of a key database into a file
-cert	-add	Add a CA certificate from a file into a key database
	-create	Create a self-signed certificate
	-delete	Delete a CA certificate
	details	List the detailed information for a specific certificate
	-export	Export a personal certificate and its associated private key from a key database into a PKCS#12 file, or to another key database
	-extract	Extract a certificate from a key database
	-getdefault	Get the default personal certificate
	-import	Import a certificate from a key database or PKCS#12 file
	-list	List all certificates
	-modify	Modify a certificate (NOTE: Currently, the only field that can be modified is the Certificate Trust field)
	-receive	Receive a certificate from a file into a key database
	-setdefault	Set the default personal certificate
	-sign	Sign a certificate stored in a file with a certificate stored in a key database and store the resulting signed certificate in a file
-certreg	-create	Create a certificate request
	-delete	Delete a certificate request from a certificate request database
	-details	List the detailed information of a specific certificate request
	extract	Extract a certificate request from a certificate request database into a file
	-list	List all certificate requests in the certificate request database
	-recreate	Recreate a certificate request
-help		Display help information for the IKEYCMD command

-version		Display IKEYCMD version information

IKEYCMD command-line options overview

The following table shows each option that can be present on the command line. The options are listed as a complete group; however, their use is dependent on the object and action specified on the command line.

Option	Description
-db	Fully qualified path name of a key database
-default_cert	Sets a certificate to be used as the default certificate for client authentication (yes or no). The default is no.
-dn	X.500 distinguished name. Input as a quoted string of the following format (only CN, O, and C are required): ″CN=Jane Doe,O=IBM,OU=Java Development,L=Endicott, ST=NY,ZIP=13760,C=country″
-encryption	Strength of encryption used in certificate export command (strong or weak). The default is strong.
-expire	Expiration time of either a certificate or a database password (in days). Defaults are 365 days for a certificate and 60 days for a database password.
-file	File name of a certificate or certificate request (depending on specified object)
-format	Format of a certificate (either ascii for Base64_encoded ASCII or binary for Binary DER data). The default is ascii.
-label	Label attached to a certificate or certificate request
-new_format	New format of key database
-new_pw	New database password
-old_format	Old format of key database
-pw	Password for the key database or PKCS#12 file. See “Creating a new key database” on page 138.
-size	Key size (512 or 1024). The default is 1024.
-stash	Indicator to stash the key database password to a file. If specified, the password will be stashed in a file.
-target	Destination file or database.
-target_pw	Password for the key database if -target specifies a key database. See “Creating a new key database” on page 138.
-target_type	Type of database specified by -target operand (see -type).

-trust	Trust status of a CA certificate (enable or disable). The default is enable.
-type	Type of database. Allowable values are cms (indicates a CMS key database), webdb (indicates a keyring), sslight (indicates an sslight .class), or pkcs12 (indicates a PKCS#12 file).
-x509version	Version of X.509 certificate to create (1, 2 or 3). The default is 3.

Command-line invocation

The following is a list of each of the command line-invocations, with the optional parameters specified in italics.

For simplicity, the actual Java invocation, java com.ibm.gsk.ikeyman.ikeycmd, is omitted from each of the command invocations.

```
-keydb -changepw -db <filename> -pw <password>
-new_pw <new_password> -stash -expire <days>

-keydb -convert -db <filename> -pw <password>
-old_format <cms | webdb> -new_format <cms>

-keydb -create -db <filename> -pw <password> -type <cms | sslight>
-expire <days> -stash

-keydb -delete -db <filename> -pw <password>

-keydb -stashpw -db <filename> -pw <password>

-cert -add -db <filename> -pw <password> -label <label>
-file <filename> -format <ascii | binary> -trust <enable | disable>

-cert -create -db <filename> -pw <password> -label <label>
-dn <distinguished_name> -size <1024 | 512> -x509version <3 | 1 | 2>
-default_cert <no | yes>

-cert -delete -db <filename> -pw <password> -label <label>

-cert -details -db <filename> -pw <password> -label <label>

-cert -export -db <filename> -pw <password> -label <label>
-type <cms | sslight> -target <filename> -target_pw <password>
-target_type <cms | sslight | pkcs12> -encryption <strong | weak>

-cert -extract -db <filename> -pw <password> -label <label>
-target <filename> -format <ascii | binary>

-cert -getdefault -db <filename> -pw <password>

-cert -import -db <filename> -pw <password> -label <label>
-type <cms | sslight> -target <filename> -target_pw <password>
-target_type <cms | sslight>

-cert -import -file <filename> -type <pkcs12> -target <filename>
-target_pw <password> -target_type <cms | sslight>

-cert -list <all | personal | CA | site> -db <filename>
-pw <password> -type <cms | sslight>

-cert -modify -db <filename> -pw <password> -label <label>
-trust <enable | disable>

-cert -receive -file <filename> -db <filename> -pw <password>
-format <ascii | binary> -default _cert <no | yes>

-cert -setdefault -db <filename> -pw <password> -label <label>

-cert -sign -file <filename> -db <filename> -pw <password>
-label <label> -target <filename> -format <ascii | binary>
-expire <days>
```

```
-certreq -create -db <filename> -pw <password> -label <label>
-dn <distinguished_name> -size <1024 | 512> -file <filename>

-certreq -delete -db <filename> -pw <password> -label <label>

-certreq -details -db <filename> -pw <password> -label <label>

-certreq -extract -db <filename> -pw <password> -label <label>
-target <filename>

-certreq -list -db <filename> -pw <password>

-certreq -recreate -db <filename> -pw <password> -label <label>
-target <filename>

-help

-version
```

User properties file

In order to eliminate some of the typing on the Java CLI invocations, user properties can be specified in a properties file. The properties file can be specified on the Java command-line invocation via the -Dikeycmd.properties Java option. For Windows platforms, a sample properties file, ikminit_hod.properties, is supplied in *your_install_directory*\bin, where *your_install_directory* is your Host On-Demand installation directory. For AIX platforms, this file is supplied in *your_install_directory*/bin. These installation directories contain the default setting for Host On-Demand.

Appendix D. Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.
```

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or region or send inquiries, in writing, to:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan
```

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

```
IBM Corporation
Department T01
Building B062
P.O. Box 12195
Research Triangle Park, NC 27709-2195
U.S.A.
```

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee. The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Appendix E. Trademarks

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

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

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation.

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

Printed in U.S.A.

SC31-6301-00