Getting Started

IBM WebSphere Host On-Demand Version 5.0

Before using this information and the product it supports, read the general information in Notices.

First Edition (September 2000)

This edition applies to Version 5.0 of IBM (R) Host On-Demand (program number 5648-D70) and to all subsequent releases and modifications until otherwise indicated in new editions.

This book is intended to help you plan for the installation and configuration of Host On-Demand V5.0.

Introducing Host On-Demand

The browser-based access of IBM Host On-Demand Version 5 gives you a simple way to reach critical host 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, where ever 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.

Support for TN3270E, TN5250, VT52/100/220 and IBM CICS Java Gateway access provides a single interface to key host data. 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.″

Using 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 NT V6 or later, or IBM Communicationn Server for OS/390 V2.6 or later - for authentication. Host On-Demand can also integrate the SSL client authentication with IBM Vault Registry. This allows you to benefit from

industry standard public key infrastructure (PKI) methods. Users request a certificate from Vault Registry, which manages, maintains and ensures certificate validity.

Database On-Demand is included with Host On-Demand to provide access to DB2 information stored on AS/400 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 AS/400 databases through a JDBC driver.

Host On-Demand is multilingual and is available in 22 languages, including double-byte character set 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.

Host On-Demand is shipped on four CDs: one for the AS/400; one for UNIX; one for Windows, OS/2 and Novell; and one for the toolkit. It is also available on tape as a System/390 (TM) program product.

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

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

Why use Host On-Demand?

There are a number of reasons why you would want to use Host On-Demand:

A cost-effective approach

You can save money in product deployment and maintenance by installing Host On-Demand on a Web Server, eliminating the need to manage individual user desktops. Users can connect directly to a host system, such as an IBM AS/400 system or an IBM S/390 system, eliminating the need for extra hardware and software required by three-tier solutions. Host On-Demand can be installed on nearly any server platform, accommodating various size organizations and branch offices.

Host On-Demand uses a Java applet, which helps to reduce your software maintenance costs and allows you to centrally manage groups and users. 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 receive the upgrade the next time they request the applet. And server maintenance is less complex with Web-based remote configuration and administration.

Create new e-business applications

Host On-Demand provides a rich tool set to deliver custom e-business applications that meet your specific business needs. These tools include the Host Access Class Library API, Host Access Beans for Java and ActiveX controls.

The Host Access Class Library API provides access to 3270, 5250 and VT data streams. These class libraries allow you to use mission-critical information in new ways, such as integrating data from one application into another.

Host Access Beans for Java provides host connectivity and emulator functions through simple, component-based development tools, like IBM Visual Age for Java. You can use these beans to rapidly create custom applications that allow you to deliver the specific functions you want to include in your host access applications. These object oriented beans help you minimize development efforts through software reuse. Application developers who are familiar with ActiveX can use IBM Host Access Controls - a set of ActiveX controls used to provide the functionality found in Host Access Beans for Java.

Connect directly to any Telnet server

Emulation function is contained in the client applet, eliminating the need for a middle tier server, which is both 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. The Telnet connection can be changed as often as your requirements for new data change. You can access an unlimited number of host sessions concurrently. Because no middle-tier server is required, you are not restricted by its capacity.

Manage large numbers of users

Access to Host On-Demand applets is controlled through defined users and groups. Once users and groups are defined, you can configure groups instead of individual users. For example, you can define sessions a for group, which each member of that group inherits. This reduces configuration and administration work. You can also permit users to create their own ID's, so large numbers of users can manage themselves.

Users can save their session configurations, macros, and keyboard and color mappings on the Host On-Demand server and retain those settings whenever they log on. Configurations can be shared, managed and distributed easily among groups and users. Session configurations can be made available to users by exporting the sessions to a network drive. Users easily import them into their configured sessions window.

As an alternative to the built-in Host On-Demand configuration server, you can use an LDAP server to store Host On-Demand configuration information. This includes LDAP storage of all user, group and session configuration information, like keyboard mappings, macro definitions, and session parameters. A migration facility is also provided to migrate existing Host On-Demand profiles into LDAP.

What's new in Version 5

Many new functions and enhancements have been added to Version 5:

Componentization
: Divides Host On-Demand Version 5 into ″components″ that are equivalent to the major features of the product. Administrators can choose to deploy the cached client containing just the features desired, for a dramatically smaller download.

Smart Cache
: Enables updates to the Cached client to download in the background,

while the older cached code is used for the current session. Once the Web browser is restarted, the updated cached code is used. This results in zero idle time for Host On-Demand users. In addition, the smart cache offers an installation status bar, so users see the progress of downloads. The Smart cache also offers a component-level check and update that works with the Componentization function to automate code distribution based on administration policies. See cached client in the Host On-Demand online help for more information.

Host On-Demand Configuration Servlet
Includes an optional servlet to eliminate configuration-specific ports to reduce firewall issues. This configuration servlet, when used with a Web application server such as WebSphere Application Server, allows Host On-Demand to use the HTTP or HTTPS ports exclusively for configuration traffic (a telnet port is still required for host connectivity). Administrators can easily deploy Host On-Demand across the extranet with no firewall restrictions. See configuring the configuration servlet in the Host On-Demand online help and Installing the configuration servlet in this guide for more information.

Deployment Wizard
Introduces a new, wizard-driven administration tool that eases planning and configuration of Host On-Demand sessions, administration options and deployment methods. The Deployment Wizard uses an intelligent decision structure to guide administrators to deploy Host On-Demand sessions, to deploy previous ″session2.html″ options, and to use new deployment options in Host On-Demand Version 5. See deployment wizard in the Host On-Demand online help for more information.

Policy Management and Feature Disable
Allows administrators to control which features are available to each user. Administrators use the graphical user interface to completely disable any feature in Host On-Demand. Disabling features reduces user errors, minimizes helpdesk workload, or controls security issues. For more information, see disabling functions in the Host On-Demand online help.

Express Logon
Allows a user running a 3270 client session to log on to a host system without entering a user ID and password. Express Logon sends Digital Certificates in place of userids and passwords to RACF through the IBM Communications Server on AIX, NT, OS/2 or OS/390, in place of user IDs and passwords. This reduces the time an administrator spends spends maintaining host user IDs and passwords. This also reduces the number of user IDs and passwords that users need to remember. For more information regarding Express logon, see Express logon in the Host On-Demand online help.

AIX Installation
Provides an automated installp installation program for AIX users, making deployment of the Host On-Demand program and maintenance updates fast and simple. For more information, see Installing on AIX in this guide.

Printer Definition File Support in Windows (select printer)
Allows a user to access a printer from a Host On-Demand Windows client with a host print session PDT (3270) or Model (5250). This reduces the workload for a user, who simply chooses an appropriate local printer for the current environment. The required PDT or Model is selected automatically. See selecting a Windows printer to use with a host printer session in the Host On-Demand online help for more information.

Improved Color Remap

Models the color remap panel from IBM Personal Communications to help reduce the amount of training required for migration from Personal Communications to Host On-Demand. Host On-Demand Version 5 supports an attribute-level color remap for greater functionality, while preserving the simpler color remap from previous Host On-Demand versions.

Improved Key Remap

Provides a more extensive panel to see which keys are mapped and what options are available. Host On-Demand Version 5 supports the ability to map:

- All shift states
- Macros to keys
- Strings to keys
- Java applets to keys
- Menu shortcuts to different keys

See remapping keyboards in the Host On-Demand online help for more information.

Multiple Session Launch Support

Adds the ability to launch multiple sessions simultaneously, including sessions from multiple hosts, from one icon. See creating a multiple session icon in the Host On-Demand online help for more information.

Paste Improvements

Includes field-wrap, line-wrap and other improvements that offer greater flexibility when pasting from other applications.

Improved Error and Status Indicators

Provides more meaningful messages on the status line which explain the error or any action that needs to be taken. This function slso provides hotlinks to help on specific messages to reduce helpdesk support load.

Improved Menu Usability

Provides a more usable menu structure with consistent terminology and layout with other Windows applications, including Personal Communications. Menu shortcut keys are available for commonly used functions.

Toolkit Package

The Host Access Beans, Host Access Class Library API, and Host Access Controls are located on a separate CD with its own installation. This provides the ability to create Host Access applications more easily on the platform of your choice. See Appendix D: Host access toolkit in this guide for more information.

Code Page Enhancements

Increases the code page table support to include all the code pages that Personal Communications supports. See National language support in this guide for more information.

Code pages added:

- 1137 (Hindi 5250 only)
- 1153 (Latin 2 Euro)
- 1154 (Cyrillic Euro)
- 1155 (Turkey Euro)

- 1156 (Baltic Euro)
- 1157 (Estonia Euro)
- 1158 (Cyrillic Ukraine Euro)
- 1160 (Thai Euro)
- 1364 (Korea Euro)
- 1371 (Taiwan Euro)
- 1390 (Japan Katakana Euro)
- 1399 (Japan Latin Euro)

Code pages modified to enable the Euro currency symbol:

- 420 (Arabic)
- 424 (Israel)
- 803 (Israel)
- 875 (Greece)

AS/400 Database On-Demand and File Transfer Proxy Server Support
Enables both Database On-Demand and file transfer to use the same default port of 3470 through a firewall, so only one port needs to be opened on the firewall.See configuring an OS/400 proxy server in the Host On-Demand online help for more information.

AS/400 Database On-Demand and File Transfer Enhanced SSL Support
Enables both Database On-Demand and file transfer to provide secure connections by encrypting the data exchanged between the host and client, and by using server authentication. See Appendix C: Configuring SSL capability for clients on AS/400 in this guide for more information.

Enhanced Non-Programmable Terminal User Interface (ENPTUI) Support
Supports 5250 enhanced features, including:

- selection fields
- scroll bar field
- continued and edit mask entry field
- cursor progression entry field
- highlighted entry field
- pointer device selectable field
- word wrap field
- pop-up window
- menu-bar selection cursor in selection fields and highlighted entry field
- cursor movement to input-capable positions
- cursor-sensitive scrolling within a selection field
- application programmable mouse buttons

Blink Attribute
Adds support for the 3270 and 5250 Blink attribute. Also provides support for a similar VT blink attribute.

VT 220 Enhancements
The Host On-Demand VT support is augmented to include:

- Greater-than-24-line support: Host On-Demand now supports an additional eight modes. These modes are 36, 48, 72, and 144 rows with 80 or 132 columns for each new row setting. The default remains 24 lines.
- Scrolling

- VT Print (print pass-through): Allows a VT-emulation user to print without being physically attached to a local printer.
- Full 220 specification compliance

Telnet-negotiated Security
Allows a Telnet session to begin as a non-secure session, then negotiate a secure session as defined in the IETF INTERNET-DRAFT "TLS-based Telnet Security." Communications Server/390 Version 2 Release 10 Telnet server supports this function. This draft defines extensions to Telnet that allow TLS to be negotiated over a Telnet connection. Host On-Demand negotiates to SSL Version 3. Host On-Demand does not support TLS security itself, as that is not yet an accepted standard. See Telnet-negotiated security in the Host On-Demand online help for more information.

Single Customizable Service Manager Port
Eliminates one of the configuration ports needed in Host On-Demand Version 4, and optionally eliminates of all Host On-Demand configuration-specific ports to alleviate firewall issues. When used with the Configuration servlet, this function allows Host On-Demand to use the HTTP or HTTPS ports exclusively for configuration traffic (a Telnet port is still required for host connectivity). See changing the Service Manager port in the Host On-Demand online help for more information.

Native Authentication
Enables users to logon to Host On-Demand using the same password they use when logging onto Windows NT, Windows 2000, AIX or OS/390. The operating system performs user authentication instead of the server. If you already have user IDs and passwords defined on Host On-Demand, you can install the native platform authentication service and select either Host On-Demand server authentication or native authentication for each user. Advantages of native authentication include reducing the time an administrator spends maintaining host user IDs and passwords, and reducing the number of user IDs and passwords that users need to remember. See native authentication in the Host On-Demand online help for more information.

Java 2 Platform Support
Provides Java 2 compatibility for development using Host On-Demand's Java Beans and Host Access Class Library.

Hindi Support
Provides Hindi support for 5250 emulation sessions, which includes mapping keyboard keys to Hindi characters, character rendering, file transfer, and printing of Hindi Characters displayed on the screen.

Bidi and Thai Support
Provides support for bidirectional character sets used in Hebrew and Arabic languages and provides Thai in support in VT mode.

Planning for Host On-Demand

- Before installing Host On-Demand
- Supported server operating systems
- Disk space requirements
- Supported browsers
- Packaging

Before installing Host On-Demand

Below are some general software requirements and information to help you make configuration decisions before installing Host On-Demand. Check the installation section in this Getting Started guide for specific software requirements for your operating system; read the readme for late breaking information; and read the Basic Configuration Steps for more detailed information about configuring Host On-Demand after installation.

Install a JDK, Web server and, optionally, a servlet engine
Use the installation section in this guide for supported JDK, browser, Web server and servlet engine levels, as well as required disk space.

Determine directory structure for Host On-Demand installation
The installation instructions, and automated installations, assume a certain directory structure. In most cases these defaults should work fine. Review the directory structure in the installation section in this guide before installing. If you change the default directory structure, keep your changes in mind when following the installation instructions.

Select the Service Manager port
During the Windows NT, 2000 and the graphical AIX installation, you are asked to select a Service Manager port. The default port is 8999 and is usually a good port (the Service Manager port is automatically set to 8999 during installation on operating systems other than NT and AIX). Check your operating system documentation to see if this port is in use. If it is in use, change the port. Make a note of the new Service Manager port.

Choose to use the configuration servlet
During the Windows NT, 2000 and the graphical AIX installation, 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. The configuration servlet allows client applets to communicate with the configuration server through a firewall without opening any additional ports on the firewall. The configuration servlet can be installed manually on the other operating systems, and for web and application servers that are not recognized by the installation program. See installing the configuration servlet in this guide for more information.

Decide what security levels to set
Access to a Host On-Demand server requires a user ID and optional password (even for shared accounts and customized HTML). Host systems usually also require a user ID and password to log on. Unless your Web server is configured for SSL, this information is **not** encrypted; it could be read by a third party. The configuration information the Service Manager communicates to sessions (such as user preferences) also is **not** encrypted. If your users are accessing Host On-Demand and host data from within your intranet, this default security setup might be enough. If you have users on the Internet accessing Host On-Demand and data on your intranet, however, you may want additional security. You can configure your Web server to use SSL, so that the data stream from you Web server to your browser is encrypted. See you Web server documentation for more information about configuring your Web server for SSL. Once the client is loaded in a browser, however, it communicates directly with the host. You may be able to configure Host On-Demand to provide SSL security to your host sessions.

- If the Telnet server supports SSL, the clients can be configured to use SSL also. See your Telnet server's documentation for more information about configuring SSL on the Telnet server, and see security in the Host On-Demand online help for more information about configuring a client to connect to a secure Telnet server.
- If your Telnet server does not support SSL, and you are running Host On-Demand on Windows NT or AIX, you can configure the Host On-Demand Redirector to provide SSL support. The Redirector acts as a transparent proxy between the client and the Telnet server by using port remapping. It can encrypt data between the client and itself, between itself and the host, or both between the client and itself and between itself and the host. See adding a host to the Redirector in the Host On-Demand online help for more information.
- If you want session configuration information to be encrypted, you can configure sessions to use the configuration servlet over HTTPS (after configuring your Web server for SSL) instead of communicating directly with the Service Manager. See installing the configuration servlet 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.

You can set these additional security options once SSL is enabled:

TLS-based Telnet Security
: You can allow the security negotiations between the client and the Telnet server to occur on the established telnet connection for Host On-Demand 3270 display and printer sessions, if the Telnet server supports this option. See Telnet-negotiated security in the Host On-Demand online help for more information.

Server authentication
: Encrypting the data exchange between the client and the server does not guarentee 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 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 allowing 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 SSL and client authentication. See Express logon in the Host On-Demand online help for more information.

Native authentication
You can allow users to logon to Host On-Demand using the password they use when logging onto Windows NT, AIX or OS/390. User authentication is performed by the operating system and not the server. See native authentication in the Host On-Demand online help for more information about installing native authentication and configuring clients to use native authentication.

Decide which data store to use for group, user and session information
Each Host On-Demand server uses its own private data store to store group, user and session information. This information cannot be shared among other Host On-Demand servers or applications. If you need to share group, user and session information among Host On-Demand servers and other applications, you may want to use a Lightweight Directory Access Protocol (LDAP) directory server instead of the default private data store. See installing LDAP support in this guide for more information about installing LDAP support and configuring Host On-Demand to use an LDAP directory. If you have a previous version of Host On-Demand installed, or have just recently installed Host On-Demand V5, you can migrate from the private date store to an LDAP directory. Because there are differences in the way the private data store and an LDAP directory store the information, you may lose some information if any of your users belongs to more than one group. Host On-Demand's private data store is not hhierarchical so users can belong to more than one group. An LDAP directory is hhierarchical so users can only belong to one group. When you migrate the private data store to an LDAP directory, all changes made to groups, users and sessions are stored in the LDAP directory. No updates are made to the private data store. The private data store is not deleted, so if you need to switch back to using the private data store, you can do so, but no updates made in the LDAP directory are reflected in the private data store. If you have a pre-existing LDAP directory defined, you may be able to use it. It may require some special programming, so that Host On-Demand can add information it needs to the LDAP directory.

Choose the clients to configure for use
The emulator clients most often used include the Download client, the Function On-Demand client, the Cached client, and the Locally-installed client. Which clients you configure depend on the needs of your users. The Download client, and the smaller Function On-Demand client, are downloaded from the server each time they are used. The Download client is the standard client and it provides all the Host On-Demand client functions except problem determination. Function On-Demand only downloads basic functions initially. Other functions are downloaded as needed. These clients perform best when download time is not a factor and connectivity is predictable, such as through a LAN. If long download times and unpredictable connectivity are factors for you, such as when users connect with slow dial-up ttelephonelines, use the Cached client or the Locally installed client. The Host On-Demand 5.0 Cached client is only downloaded the first time it is run. After that, it checks for updated components on the server every time it is run. If any components on the server are newer than those in cache, only the newer components are

downloaded. You can continue to use the current level of the Cached client to connect to a host while the newer components are downloading. The Locally installed client is not downloaded from a server at all. It is installed on a local disk, and once you configure it, connects directly to a host. Since it is installed to a local disk, it must be reinstalled when upgrading. The remaining clients are special function clients (for example, the Database On-Demand client, New User Client, Remove Cached Client, and Administration client), printer session clients, and variations of the emulator clients that allow you to use them along with the Cached client or do problem determination. See loading the Host On-Demand clients in this guide for more information about these clients.

Install and configure Host On-Demand

Follow the installation instructions in this guide to install Host On-Demand 5.0, then see Basic Configuration Steps in the Host On-Demand online help for more detailed information about configuring Host On-Demand so users can access host sessions. Briefly, you will perform these steps:

1. Open the Administration window.
2. Change the Admin's password.
3. Create groups and sessions for the groups.
4. Create users and add them to groups.
5. Tell users how to access the sessions.

Supported server operating systems

For updates to this information, refer to the readme file.

A Host On-Demand server can be installed on the following operating systems:

- Windows NT 4.0 with SP5 or later and Windows 2000
- AIX (R) Version 4.2.x, 4.3.3, and 4.3.4
- OS/2 (R) Warp Version 4 and Warp Server for e-Business 4.5
- Novell NetWare Version 4 and 5
- Sun Solaris 2.6 and 2.7
- OS/400 (R) Version 4 Release 3, Version 4 Release 4, and Version 4 Release 5
- HP/UX 10.20
- RedHat Linux Version 6 Release 2 or later

Host On-Demand V5 does not work with the Gnome 1.0 desktop, using the default window manager, Enlightenment. You must upgrade to Gnome 1.2 or later and use the new default window manager, SawFish.

- SUSE 6.4
- OS/390 (R) Version 2 Release 5, Version 2 Release 6, Version 2 Release 7, Version 2 Release 8, Version 2 Release 9 and Version 3 Release 10
- Caldera 2.3
- TurboLinux 6.0
- Unixware 7
- Windows Terminal Server Version 4

Disk space requirements

These requirements are based on a typical installation and are only estimates. Sizes can vary by operating system and which languages are installed.

- Windows NT or Windows 2000 - 236MB (English only. Add 4 to 8MB for each additional language)
- AIX (installp image) - 190MB (English only. Add 4 to 8MB for each additional language. Includes the additional security files)
- UNIX (Solaris, HP-UX or Linux) - 84MB (English only. Add 4 to 8MB for each additional language)
- AS/400 - 300MB DASD
- OS/2 and Novell - 207MB

Supported browsers

Browsers change from time to time. For the most up-to-date information, refer to the readme file and to the Host On-Demand Web site. Use the following browsers 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 or 4.7.x (Windows 95, 98, 2000, NT, UNIX)
- Netscape Navigator 4.6.1 for OS/2
- Microsoft Internet Explorer 4.01 with SP1, 5.0 or 5.1 (Windows 95, 98, 2000, NT). JVM level must be 3165 or higher.

Packaging

Host On-Demand is provided on 4 CDs: one CD for OS/2, Novell and Windows; and one CD for UNIX (AIX, HP-UX, Linux and Solaris). This includes the code, publications, helps, and other files for all the supported languages. Separate CDs are provided for OS/400 and the toolkit.

Installation formats provided on the CDs include:

- InstallShield for Windows NT, Windows 95, Windows 98 and Windows 2000
- ZIP for OS/2, and NetWare
- installp for AIX
- TAR for Linux, Solaris, and HP/UX
- Separate CD for AS/400
- Separate CD for the toolkit

For OS/390, Host On-Demand is provided on three different media:

- 6250 tape
- 3480 cartridge
- 4 millimeter cartridge

Installing Host On-Demand

The 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 the Host On-Demand server

The installation steps are different for each operating system.

- Installing on Windows NT or Windows 2000
- Installing on OS/2
- Installing on Novell NetWare
- Installing on AIX
- Installing on UNIX
- Installing on OS/400
- Installing on OS/390

Installing on Windows NT and Windows 2000

An NT Web server is required to automatically install Host On-Demand on Windows NT or 2000. The following Web servers are recognized and automatically configured:

- IBM Internet Connection Server
- Microsoft Web Servers:

Internet Information Server 3 and 4
Peer Web Services
Personal Web Server

- Lotus Go, Domino, and Domino Go
- IBM HTTP Server
- Netscape Enterprise Server

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

Installing Host On-Demand using InstallShield

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

You must be a member of the Administrators group.

1. If autoplay is enabled on your Windows NT or 2000 server for your CD drive, insert the CD and wait for the start window. Otherwise, insert the CD and run the `setup.exe` program in the win32 directory.
2. Click Install Product.
3. 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 Manger'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, which was the default configuration for Host On-Demand V4.0. See installing the configuration servlet in this guide for more information.

4. If you have not already done so, read the readme file (available in the last window after installation).
5. 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.
6. Restart the Web server.
7. Load the `HODMain.html` , located in the `hostondemand\HOD` directory, into your browser. This page contains links to all the Host On-Demand clients, the readme file, and basic configuration steps for configuring the Host On-Demand server.
8. Click Start > Programs > IBM Host On-Demand > Administration > Getting Started.

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. 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 5.0, 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=v5.00.000

File=Log File

[Application]

Name=\Host On-Demand Server

Version=5.00.000

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 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 code.
- There is not enough space on specified target drive to install the code.
- You are installing/uninstalling Host On-Demand and you are not logged onto the target machine with Administrator authority.
- There is an error in the syntax of the `setup.exe` command.

Installing on OS/2

The following are required to install Host On-Demand on an OS/2 server:

- Hard disk configured for HPFS
- OS/2 Web server, such as Lotus Domino Go Webserver for OS/2
- OS/2 Java Development Kit V1.1.8 or later. You can obtain the latest JVM level from one of the following sites:

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

  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. Depending upon which JVM you installed, 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.

If you have previously installed Host On-Demand and have changed `/hostondemand/lib/NSMprop` or changed or created `/hostondemand/hod/config.properties` , you must back up these files before installation, then restore them after installation. The files are ooverwrittenduring 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\hod50srv.zip
```

   where:
   - *unzip* is your unpacking program (such as `UNZIP.EXE`). It must support long filenames
   - *[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\hod50www.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.

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 command to your `startup.cmd` file so that the Service Manager starts automatically when the workstation boots. If you do, remember to include logic to change directory to the `\hostondemand\lib` subdirectory before the command runs.

11. Restart the Web server.
12. Load `HODMain.html` , located in the `\hostondemand\HOD` directory, into your browser.
    - Click readme - Please! to see information that was not included here or the Help.
    - Click Basic configuration steps to help you get started with configuring the Host On-Demand server.

Installing on Novell NetWare

The following are required to install Host On-Demand on a Novell server:

- Novell NetWare 4.*x*
- Novell Web Server
- Novell Java Development Kit V1.1.8 or later

To obtain the Novell JDK, go to `http:\\www.developer.novell.com` . The JDK must be configured for long-filename support.

If you have previously installed Host On-Demand and have changed `/hostondemand/lib/NSMprop` or changed or created `/hostondemand/hod/config.properties` , you must back up these files before installation, 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. From a client workstation, map a drive to the `SYS:` volume of the Novell server.
2. Mount the `SYS:` volume.
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\hod50srv.zip
```

   where:
   - *unzip* is your unpacking program (such as `UNZIP.EXE`). It must support long filenames.
   - *[cd_rom]* is the CD-ROM drive letter.
   - *zip* is the directory on the CD.
7. Change to `SYS:\web\docs` . This directory is usually published (made available to client users who access the server through a browser) automatically. If the `\web\docs` directory does not exist, create a publish directory, for example `HOD` , change to that directory, and go to Step 10.
8. Create a 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.

9. Run the following command to extract the files:

```
unzip [cd_rom]:\zip\hod50www.zip
```

10. If you unpacked `hod50www.zip` into `SYS:\web\docs` as suggested above, the `HOD` directory is automatically published, because it is a subdirectory of the default published directory, `SYS:\web\docs` . If you unpacked the file anywhere else, publish that directory (make it available to client users who access the server through a browser). Refer to the Web server documentation for information about how to do that.
11. Reboot the server.
12. From the server console, run the command `load java` to start the Java NLM.
13. 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. Change directory to the `\hostondemand\lib` subdirectory.
    b. 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 filename to the eight-dot-three format.
    c. Edit `NCServiceManager-Novell.ncf` (or the eight-dot-three format of the file) to reflect the directory paths that are correct for your workstation.
    d. 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.

14. Restart the Web server.
15. Load `HODMain.html` , located in the `\hostondemand\HOD` directory, into your browser.
    - Click readme - Please! to see information that was not included in here or the Help.
    - Click Basic configuration steps to help you get started with configuring the Host On-Demand server.

Installing on AIX

To install Host On-Demand on AIX, the following are required:

- AIX Web server
- JDK 1.1.8 or later

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. Mount the CD-ROM drive and insert the CD.
2. Start the installation program by changing to the root directory of the CD, type `setupaix.sh` and press Enter.
3. Click Install Product.
4. 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 during the install or later. For more information about changing the Service Manager port, see Changing the Service Manger'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, which was the default configuration for Host On-Demand V4.0. See installing the configuration servlet in this guide for more information.
5. If you have not already done so, read the `readme` file available in the last window. Click finish to end the installation.
6. 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 Publish directory to the Web. Refer to the Web server documentation for information on how to publish the directory.
7. Restart the Web server.

If you are using WebSphere Application Server 3.0.02 with your Web server, you must stop and restart it.

8. Load `HODMain.html` , located in the `/usr/opt/hostondemand/HOD` directory, into your browser. This page contains links to all the Host On-Demand clients, the readme file, and basic configuration steps for configuring the Host On-Demand server.

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\AIX 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.
/fully/qualified/log_file_name	Defines the name for a log or trace file, which can be used to debug installation problems. The default name is install.log, but 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.

To install in silent mode using the `install.script` from the CD:

```
/cdrom/instmgr/installaix.sh -p /cdrom/instmgr/AIX/install.script
```

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

```
/cdrom/instmgr/installaix.sh -p /cdrom/instmgr/AIX/install.script
/tmp/install.log
```

To record a response file:

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

To playback the response:

```
/cdrom/instmgr/installaix.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 4.0, 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 types.

Installing on UNIX (Solaris, HP/UX, and Linux)

To install Host On-Demand on Solaris, the following are required:

- Solaris Web server
- JDK V1.1.8

To install Host On-Demand on HP/UX, the following are required:

- HP Web server
- JDK V1.1.8

To install Host On-Demand on Linux, the following are required:

- Linux Web Server
- JDK V1.1.8

Host On-Demand V5 does not work with the Gnome 1.0 desktop, using the default window manager, Enlightenment. You must upgrade to Gnome 1.2 or later and use the new default window manager, SawFish.

Obtain the latest JDK for UNIX from one of the following sites:

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

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

To install the Host On-Demand server on a UNIX workstation, follow the steps below. These examples assume that you are installing Host On-Demand in the /usr/opt 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. 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. Tar files are located in the /cdrom/tar directory. Untar the files from hod50srv.tar to the server directory.
5. Create a publish directory, for example, HOD . The publish directory contains files that must be made available to client users who access the server through a browser.
6. Untar hod50www.tar into the HOD directory. 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:

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

7. In this example, assume that the tar files are in the /cdrom/tar directory. These commands create the /usr/local/hostondemand and /usr/local/hostondemand/HOD directories and install the files.

```
cd /usr/local
mkdir hostondemand
cd hostondemand
tar -xf /cdrom/tar/hod50srv.tar
mkdir HOD
cd HOD
tar -xf /cdrom/tar/hod50www.tar
```

8. 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.
9. 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.

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

10. Restart the Web server.
11. Load HODMain.html , located in the hostondemand/HOD directory, into a browser.
    - Click readme - Please! to see information that was not included here or in the Help.
    - Click Basic configuration steps to help you get started with configuring the Host On-Demand server.

Installing on OS/400

The following are required for installing Host On-Demand on an AS/400 server:

- TCP/IP Connectivity Utilities for AS/400 (5769TC1)
- One of the following AS/400 HTTP servers: 5769DG1, 5769NCE, 5769NC1 or 5769LNT
- Java Developer's Kit (5769JV1)
- AS/400 Java Toolbox (5769JC1)
- QShell Interpreter (5769SS1 Option 30)

- 256MB memory or more. Refer to the AS/400 Performance Capabilities Reference Web page `http://publib.boulder.ibm.com/pubs/html/as400/onlinelib.htm` for additional information about the impact of additional memory and Java performance
- Recent cumulative service is recommended. Refer to the AS/400 Fixes, Downloads and Updates Web page `http://as400service.rochester.ibm.com/`.

You must have `*SERVICE`, `*JOBCTL` and `*ALLOBJ` authority.

To install Host On-Demand V5:

1. Sign on to the AS/400 with the `QSECOFR` user profile (or user profile with equivalent security authorities).
2. If Host On-Demand (5648D70) has previously been installed, issue the following AS/400 command to shutdown the Service Manager:

```
ENDHODSVM
```

3. Place the Host On-Demand for AS/400 CD in the AS/400 CD drive.
4. Type the following AS/400 command:

```
RSTLICPGM LICPGM(5648D70) DEV(OPT01)
```

   This command will process for 10-45 minutes, depending upon the configuration of the AS/400.
5. For each additional OS/400 secondary language that you would like to provide full help text support for, type the following AS/400 command:

```
RSTLICPGM LICPGM(5648D70) DEV(OPT01) LNG(xxxx) TYPE(*LNG)
```

   Where *xxxx* is the language code from the list below. This step is optional, and could be performed later.

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
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

6. If you have previously installed IBM Host On-Demand Screen Customizer Runtime for AS/400 (5648D01), must install the new version of that product or reinstall the current version at this time. Refer to the installation manual for Host On-Demand Screen Customizer.
7. If you want the Host On-Demand Service Manager to automatically start after an IPL (when QSYSWRK is started), type the following AS/400 command:

```
CHGHODSVM AUTOSTART(*YES)
```

8. To view the status of the Host On-Demand Service Manager, type the following AS/400 command:

```
WRKJOB QHODSVM
```

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

Configuring the AS/400 HTTP server

The following commands assume that you are using the `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. Refer to the AS/400 Webmaster's Guide `http://as400bks.rochester.ibm.com` for additional information.

1. Stop the Web server:

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

2. Configure the Web server:

```
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:

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

6. If want the Host On-Demand Service Manager to automatically start after an IPL (when QSYSWRK is started), type the following AS/400 command:

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

7. Load http://*server_name*/*hod_alias*/hodmain.html (where *server_name* is the name of your server and *hod_alias* is the directory you set in step 3 above) to verify that the Web server can serve Host On-Demand HTML pages.

Configuring, starting and stopping the Host On-Demand Service Manager on AS/400

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

```
GO HOD
```

The following commands can be used from the menu or the AS/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 prestart 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 enter:

```
WRKJOB QHODSVM
```

Stop (ENDHODSVM)

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

Problem Determination

If Host On-Demand will not run, it may be that the Service Manager did not start correctly. In this case:

1. Choose option 4 from the menu.
2. Wait a few minutes.
3. Review the list of Java classes that were not loaded.
4. Use the `WRKLNK` command to locate the missing classes.
5. Adjust the Java classpath settings using the `CFGHODSVM` command.
6. Repeat the process until all errors are fixed.

Installing on OS/390

For instructions about installing Host On-Demand on OS/390, refer to the Program Directory supplied with the OS/390 Program Product.

Installing the configuration servlet

The 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, with Host On-Demand 5.0, 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 doesn't need to be opened for Host On-Demand.

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

During the Host On-Demand installation, the configuration servlet is automatically installed and configured on Windows NT, 2000 and AIX for recognized Web or application servers that support the Java Servlet 2.0 API. Recognized Web or application servers include:

- IBM WebSphere Application Server
- Lotus Domino Go Web Server
- IBM Domino Go Web Server

You must manually install the Host On-Demand configuration servlet for other Web servers on Windows NT and 2000 and AIX, and on all Web servers on the OS/2, Novell, AIX, Sun Solaris, HP-UX, Linux, OS/400 and OS/390 operating systems. The following instructions assume a Web server is already installed on Windows NT.

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.

To manually install the configuration servlet:

- Install Host On-Demand, without running the configuration servlet installation, to a directory such as `d:\hostondemand` .
- 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` . 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 `/hostondemand/lib` directory where you installed Host On-Demand on your server.
- 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.
- Configure the configuration servlet. If necessary, set the `ConfigServer` and `ConfigServerPort` parameters to the hostname 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.
- Publish the `HODConfig` servlet with an alias of `/servlet/HODConfig` . Refer to your Web server or servlet engine documentation for informationon 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, such as `/servlet/HODConfig/hod` .
- 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 ConfigServerURL 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 Host On-Demand online help.

Installing the AS/400 Toolbox for Java

The AS/400 Toolbox for Java is a set of Java classes that enable you to write client/server applications and applets that work with data residing on your AS/400. You can also run such applications on the AS/400 Java Virtual Machine (JVM).

The Toolbox uses AS/400 servers as access points to the system. Each server runs as a separate job on the AS/400, and each job sends and receives datastreams on a socket connection.

The access classes provide low-level access to the following AS/400 resources:

- databases via a JDBC driver or record-level access
- Integrated File System
- programs
- commands
- data queues
- print
- digital certificates
- jobs
- message queues
- users and groups
- user spaces

Graphical programming interfaces are available for:

- databases (both JDBC and record-level access)
- command call
- data queues
- integrated
- file system
- jobs
- message queues
- print
- program call
- users and groups

The following files are located on the toolkit CD (**not** the AS/400 CD):

- `jt400_all.zip` contains `jt400.zip` , `jt400.jar` , utilities files, and help and message files
- `jt400_doc_en.zip` contains the Programmer's Guide in English
- `jt400_doc_ja.zip` contains the Programmer's Guide in Japanese
- `jt400_doc_ko.zip` contains the Programmer's Guide in Korean
- `jt400_doc_zh.zip` contains the Programmer's Guide in Simplified Chinese (PRC)
- `jt400_doc_es.zip` contains the Programmer's Guide in Spanish
- `jt400_doc_zh_TW.zip` contains the Programmer's Guide in Traditional Chinese.

To install the AS/400 Toolbox for Java on your workstation, unzip the appropriate files. For example, if you want to install the code and the English version of the Programmers Guide, `unzip jt400_all.zip and jt400_doc_en.zip` .

You must use a utility that supports long filenames.

For additional information on the toolbox, see `http://www.as400.ibm.com/toolbox`.

Migrating Host On-Demand V3.0 or Host On-Demand V4.0 to Host On-Demand V5.0

Attention
For Windows NT and Windows 2000 you **must not** remove the previous release before installing Version 5. Migration is performed automatically as part of the installation process. If you remove the previous version, the migration utility will not run.

For other operating systems, migration is not necessary. All configuration information is saved. If you install Host On-Demand V5 using a server directory other than the default, you must move the private directory to the new server directory.

If you have changed `/hostondemand/lib/NSMprop` or changed or created `/hostondemand/hod/config.properties` on a platform other than Windows NT or 2000, you must back up these files before installation, then restore them after installation. The files are overwritten during the unzip or untar process on platforms other than Windows.

Removing Host On-Demand

To remove the Host On-Demand server:

Windows NT or 2000
Use Add/Remove Programs from Control Panel. If InstallSheild does not remove the `hostondemand` directory you must remove it manually.

UNIX 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`).

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

AS/400
You will need `*JOBCTL`, `*SPLCTL`, `*SERVICE` and `*ALLOBJ` authority to use this command. Logon to the AS/400 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(5648D70)` 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.

To remove the Cached client:

Load `http://` *server_name/hod_alias*`/HODRemove.html` in your browser. It immediately removes all previous versions of the Cached client from all levels of Netscape and Internet Explorer.

Using Host On-Demand with a firewall

If you are configuring Host On-Demand to go through a firewall, make sure the firewall administrator opens port 8999 internally and externally. The Service Manager listens to port 8999 by default, and the client receives configuration information directly from the Service Manager over port 8999 by default. You can customize the port the clients and Service Manager use. To customize the port, see changing the Service Manager port in the Host On-Demand online help.

In addition to port 8999, make sure the firewall administrator opens any ports that are being used for functions your clients use. For example, if you have an SSL session with the Redirector on port 5000, port 5000 must be opened for telnet traffic. The following table summarizes the ports that Host On-Demand can use.

Host On-Demand Function	Ports Used
Display emulation (5250 and 3270)	23 (telnet), 80 (http) and 8999 (config server)3
Printer emulation (5250 and 3270)	23 (telnet), 80 (http) and 8999 (config server)3
3270 file transfer	23 (telnet), 80 (http) 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)3, 449 (as-svrmap)4, 8470 (as-central)1 2 4, 8473 (as-file)1 4, and 8476 (as-signon)1 4
HODAdmin.html	80 (http) and 8999 (config server)3
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)	80 (http)
Session1.html	23 (telnet), 80 (http) and 8999 (config server)3
Session2.html	23 (telnet) and 80 (http)

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 code-page 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 AS/400 proxy server support. You will need to open the default proxy server port 3470. You can change this port.

Configuring Host On-Demand

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

Groups, users and sessions are configured through the administration window. On all operating systems you can open the Administration window by entering http://*server_name*/*hod_alias*/HODAdmin.html in your browser, where *server_name* is the name of your Web server and *hod_alias* is the alias you selected during installation. Log on with the default user ID and password of *admin* and *password*. It is recommended that you change the admin password. To change the admin paswword:

1. Click Users/Groups.
2. Select HOD (System default group).
3. Right-click the Admin user, then select Properties.
4. Type a password in the New Password field, then type it again in the Confirm Password field in the Change User window.
5. Click OK to save your changes.

On Windows NT or 2000 you can also start the administration window by clicking Start > Programs > IBM Host On-Demand > Administration > Administration Utility.

From the Administrator window, you can:

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

- View trace information for users
- Disable functions to end users

Group membership

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

User accounts

User accounts provide password-protected access to Host On-Demand. Passwords are secure during the logon process; however, IDs are not. Users can create their own accounts, if enabled in the Users/Groups window. As part of the account, session configuration information is saved, along with changes that the user makes during a session. These changes include changes to keyboard and color mapping, and to recorded macros.

Administrator account

An Administrator account is provided. The default user ID is *admin* and the password is *password*. As an administrator, you can change the ID and the password; however, you cannot delete the administrator account. You can also create additional administrator accounts. All passwords are encrypted; however, user IDs are not.

If you change the user ID or password, you must remember what you have changed. The only way to restore the default user ID and password is to reinstall Host On-Demand.

Shared user accounts

There is no specific guest user ID provided with Host On-Demand. However, you can create one or more user IDs that can be shared by several people. You can create groups for casual users, for example, by department or area. If you click the **Do not save preferences** check box when you create a shared user account, anyone using this account can change preferences while a session is running, but the changes are discarded when the user logs off. In this way, changes made by one casual user do not affect others.

Host sessions

You can configure host sessions for groups or for individual users. It is preferable to define groups, define their host sessions, and then add users to the groups. All the users in the group then have access to the sessions defined for the group, and you do not need to define sessions separately for each user. Within their own sessions, users can customize without affecting the session definitions in the groups. User preferences are saved in their accounts and do not affect the sessions of other users.

User preferences

Unless **Do not save preferences** is checked when an account is created, preferences set during a host session are saved. These include color and keyboard mapping,

macros created or changed, and the settings for the toolbars. These preferences are saved in the account of the individual user and associated with the icon for the session to which they apply. Also, if a preference is saved for a user, that preference will take precedence over the group preference. You will have to change the preference for that user. If you do not want them to override group preferences, lock or disable user preferences.

Creating and managing groups, users and sessions example

For example, carefully consider the kinds of users and types of connections they require before creating and managing groups and users. Suppose you have the following users:

- User1 and User2 who need access to Host A
- User3 who needs access to Host B and
- Manager, who requires access to all host sessions.

The connections to the host systems are:

- Host A, a 3270 session to some.hostname.com on port 23
- Host B, a 5250 session to someother.hostname.com on port 23.

To configure this example, open the administration window, then:

1. Define groups. Create GroupA for users who need access to Host A, GroupB for users who need access to Host B and GroupC for users who need access to both Host A and Host B.

Every user must be a member of at least one group, and can be a member of multiple groups; however, if you are using an LDAP server to store configuration information instead of Host On-Demand's internal configuration server, users cannot be members of more than one group.

2. Define and customize sessions for these groups. Create SessionA for access to Host A and SessionB for access to Host B. Then add SessionA to GroupA, SessionB to GroupB and both SessionA and SessionB to GroupC.
3. Define the users and add them to the groups they need to be in. Create User1 and User2, then add them to GroupA. Create User3 and add it to GroupB. Create Manager and add it to GroupC.

If there are users that have unique requirements, or you want to define a specific LU for one or more users, you must define the sessions for each user separately.

Loading the Host On-Demand clients

The Host On-Demand clients are implemented as HTML files that you load into a Web browser.

There are many ways users can load the clients:

- Load the `HODMain.html` file, located in the `/hostondemand/HOD` directory, into your browser to view links to all the available clients. You can edit the HTML file and customize its contents to suit your users and their environment. Users won't need to remember the name of the client or the name of the file that is used to load it.

- Load the full URL.

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:

```
http://name.city.yourcompany.com/hod/HOD.html
```

  will load the default Host On-Demand Download client.
- Customize your own HTML pages to launch sessions that you have configured. You can use the Deployment Wizard to create customized pages. See Deployment Wizard in the Host On-Demand online help for more information. Sample HTML pages, `session1.html` and `session2.html` , are also provided in the `/doc/samples/html` directory. These samples include examples of all HTML parameters supported by the client applets.

Let users know about the security warning that appears when using Host On-Demand. The purpose of the window is to tell users that Host On-Demand was created by **International Business Machines** and to ask whether they trust it.

Host On-Demand clients

Package	Client	HTML File
Administration Clients	Administration client	HODAdmin.html
	Administration client cached	HODAdminCached.html
	Administration client cached with problem determination	HODAdminCachedDebug.html
Emulator Clients	Cached client	HODCached.html
	Cached client with problem determination	HODCachedDebug.html
	Download client	HOD.html
	Download client with problem determination	HODDebug.html
	Download client with Screen Customizer/LE Interface	HODCustom.html
	Function On-Demand client	HODThin.html
Database Clients	Database On-Demand client	HODDatabase.html
	Database On-Demand client cached	HODDatabaseCached.html
	Database On-Demand client cached with problem determination	HODDatabaseCachedDebug.html
Utilities	Remove Cached Client	HODRemove.html
	New user client	NewUser.html
	New user client cached	NewUserCached.html
	New user client cached with problem determination	NewUserCachedDebug.html

Administration Clients

The Administration client (`HODAdmin.html`) starts the Administration window where you can:

- 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

You must add users and configure sessions for them before they can access the download clients.

Administration client cached (`HODAdminCached.html`)

This client starts the Administration client in a cached environment. Load this HTML page if you want to use the Administration client in cached environment without problem determination.

Administration client cached with problem determination (`HODAdminCachedDebug.html`)

This client also starts the Administration client in a cached environment. Load this HTML page if you want to use the Administration client in cached environment with problem determination (session logging and tracing).

Cached clients

The Cached client (`HODCached.html`) provides all the Host On-Demand functions including problem determination and the Screen Customizer. It is 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 software on the server is more recent than the software that has been cached. It so, the cached software is updated. The Cached client is recommended for users that have 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 want to remove it, you must load http://*server_name*/*hod_alias*/HODRemove.html in your browser, where *server_name* is the name of your Web server and *hod_alias* is the alias you selected during installation.

Supported browsers and operating systems

- Netscape Navigator 4.6 or 4.7.*x* (Windows 95, 98, 2000, NT, UNIX)
- Netscape Navigator 4.6.1 for OS/2
- Microsoft Internet Explorer 4.01 with SP1, 5.0 or 5.1 (Windows 95, 98, 2000, NT). JVM level must be 3165 or higher.

Installing the Cached client

There are two ways to install the Cached client. You can install it from the server, or from a local source, such as a CD or a network drive.

To install the Cached client from the server, you can either:

- Load http://*server_name*/*hod_alias*/HODCached.html
- Click on the Cached client link after loading http://*server_name*/*hod_alias*/HODMain.html.

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.

To install the Cached client from a local source:

1. Copy the following files from the *HOD* publish directory of your Host On-Demand server installation, to a network drive or put them on a CD:

```
HODCached.html (customized for a LAN or CD load)
hodlogo.gif
hodbkgnd.gif
Installer.html
Cached.js
ccversions.properties
CachedAppletInstaller.*
CachedAppletSupporter.*
CachedAppletRemover.*
sccbase.*
*.jar
*.cab
scccversions.properties
```

These next files are in subdirectories of the *HOD* 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\msgs\cached_*.class
```

2. Start the browser and open the file `HODCached.html` from the source (CD or directory). The installation begins immediately. You will see a progress bar as the client is installed, then a message asking you to restart the browser. Do so, then enter the URL for the cached client on your Host On-Demand server, not on the local source:

http://*server_name*/hod/HODCached.html

   From now on, load `HODCached.html` from the server.

With Host On-Demand 5.0 you can use new versions of `HODAdmin.html` , `HODDatabase.html` and `HODDebug.html` with the Cached client. You can load `HODAdminCached.html`, `HODDatabaseCached.html` and `HODCachedDebug.html` without first removing the Cached client.

Troubleshooting

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.

Cached client with problem determination (`HODCachedDebug.html`)

This client starts the Cached client with problem determination (session logging and tracing).

Download clients

The Download client is the standard client (`HOD.html`) , providing all Host On-Demand client function, except problem determination. Unlike the Cached client, the Download client is downloaded from the server every time you want to use it. This client has the traditional ″green screen″ interface.

Use this client if:

- You do not want to take up disk space on client machines by installing the Cached client or the Locally-installed client
- You cannot use the Cached client because you don’t have a suitable browser.
- You initial download time is not an issue.

Download client with Screen Customizer/LE Interface (`HODCustom.html`)

This is the standard client with a window-like interface provided by Screen Customizer. It is downloaded from the server each time it is used.

Download client with problem determination (`HODDebug.html`)

This client loads the standard Download client with problem determination (session logging and tracing).

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 can be configured with the traditional ″green screen″ interface, or it can be configured with the Screen Customizer/LE interface.

You can also create your own Function On-Demand client using the Deployment Wizard, specifying what functions are enabled and what functions download initially.

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

Database On-Demand clients

The Database On-Demand client (`HODDatabase.html`) provides users with a means of making Structured Query Language (SQL) requests to AS/400 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. Load this HTML page if you want to use the Database On-Demand client in cached environment without problem determination.

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

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

Remove Cached Client

The Remove Cached client (`HODRemove.html`) removes all previous versions of the Cached client from all levels of Netscape and Internet Explorer. Load http://*server_name*/*hod_alias*/HODRemove.html and it will remove the Cached client immediately.

New user clients

Users can use the New user client (`NewUser.html`) to create new accounts, if you check Allow users to create accounts in the Users/Groups window.

New user client cached (`NewUserCached.html`)

This client starts the New user client in a cached environment. Load this HTML page if you want to use the New user client in a cached environment without problem determination.

New user client with problem determination (`NewUserCachedDebug.html`)

This client starts the New user client in a cached environment with problem determination. Load this HTML page if you want to use the New user client in a cached environment with problem determination (session logging and tracing).

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. Host On-Demand uses Secure Sockets Layer (SSL) protocol to provide security for emulator sessions. SSL is an industry-standard protocol that 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 V3 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 SSL V3
- 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

A Certificate Wizard (Windows NT, Windows 95, Windows 98 and Windows 2000 only) and a graphical Certificate Management utility are provided to:

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

Using SSL

SSL is supported only on Windows NT and AIX redirectors, and on clients that have Netscape Communicator 4 or Microsoft Internet Explorer 4 or later browsers.

To use SSL on an AIX server, you must install additional files.

Host On-Demand provides secure connections between the following:

- A client and the Host On-Demand Redirector or other Telnet server that supports SSL
- Two Host On-Demand Redirectors

There are three security options that you can configure. Configuring all three provides the most security possible:

Enable SSL on client sessions
Encrypts data between the client and server

Server authentication
Provides additional server verification to the client

Client authentication
Provides client identification to the server (client must have a certificate trusted by the server)

To use server or client authentication, you must first enable SSL.

How SSL security works

SSL 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 that is used to encrypt all session data. The key is then encrypted with the server's public key and sent to the server.

SSL provides three basic security services:

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

Message integrity
Ensures that SSL session traffic does not change en route to its final destination. SSL uses 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.

An 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 SSL 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.

Certificates, encryption, and authentication

Security is controlled by certificates that act as electronic ID cards. These 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. For Host On-Demand, you can use a CA's certificate, but you can also create and sign your own. 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.

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.

To support SSL services, Host On-Demand uses two databases:

HODServerKeyDb.kdb
: Is created the first time you configure SSL for the Host On-Demand Redirector. This database contains the server's private key and certificate, and a list of CAs. Because the CAs are included in the file, they are called *well-known* or *trusted* to the Redirector. You can add certificates from other CAs (unknown CAs) and certificates that you create and sign yourself (self-signed) to this database.

CustomizedCAs.class
: Is created and updated during SSL configuration. This database contains server and CA-root certificates that are not in the well-known list and are needed by Host On-Demand clients.

Examples of when to use SSL security

Some situations where you might want to use SSL 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.

Using the Redirector

On Windows NT and AIX, the Redirector provides support for Secure Sockets Layer (SSL) security between clients and the Host On-Demand server. If a client

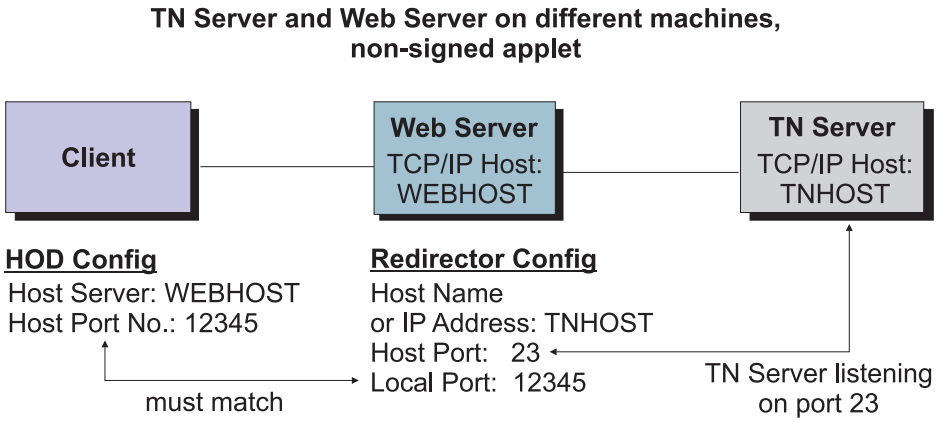
workstation is using a browser that does not support signed applets, the Redirector allows clients to connect to Telnet servers that are not installed on the same system as the Host On-Demand server.

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.

Redirectors can be connected to each other (in a cascaded configuration). In that case, SSL security is also available between the Redirectors (Windows NT and AIX only).

How the Redirector works

The following scenario shows how the Redirector works. Secure connections are possible between the client and Host On-Demand server.



The Redirector sets security for each local port. Security choices are:

- 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 - encrypts data both ways

You must enable security 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.

Telnet-negotiated security

Telnet-negotiatied 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.

It is based on INTERNET-DRAFT TLS-based Telnet Security, which defines extensions to Telnet so that Transport Layer Security (TLS) can be negotiated over a telnet connection. The TLS Protocol 1.0 allows security negotiation down from TLS 1.0 to SSL. Host On-Demand clients will always negotiate down to SSL V3, since Host On-Demand supports INTERNET-DRAFT TLS-based Telnet Security, but not TLS Protocol 1.0.

The Telnet server must support TLS-based Telnet Security for the Host On-Demand clients to use Telnet-negotiated security. At the time this book was written, Communications Server/390 version 2 release 10 was the only Telnet server that supported TLS-based Telnet Security. CS/390 documentation refers to Telnet-negotiated security as ″negotiable SSL″.;

For more information regarding Telnet-negotiated security, see Telnet-negotiated security overview in the Host On-Demand online help.

For assistance in configuring Telnet-negotiated security on a 3270 display or printer session, see configuring Telnet-negotiated security; in the Host On-Demand online help.

Sample scenarios

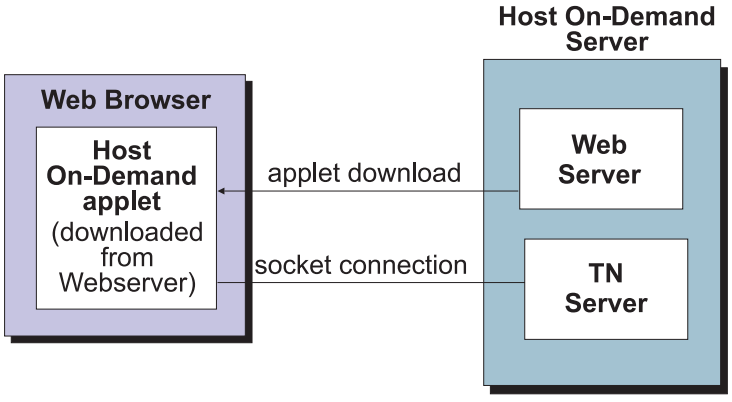
These scenarios can help you to understand how Host On-Demand works.

Server/client installations

In this environment, Host On-Demand is installed on a Web server and the client is downloaded to each workstation through a browser. The client is in the form of an HTML file.

Figure 1

If a Telnet server such as IBM Communications Server is installed on the same computer as the Host On-Demand server, clients can connect to a host system through the Telnet server. SSL may or may not be available, depending on whether the Telnet server supports it.



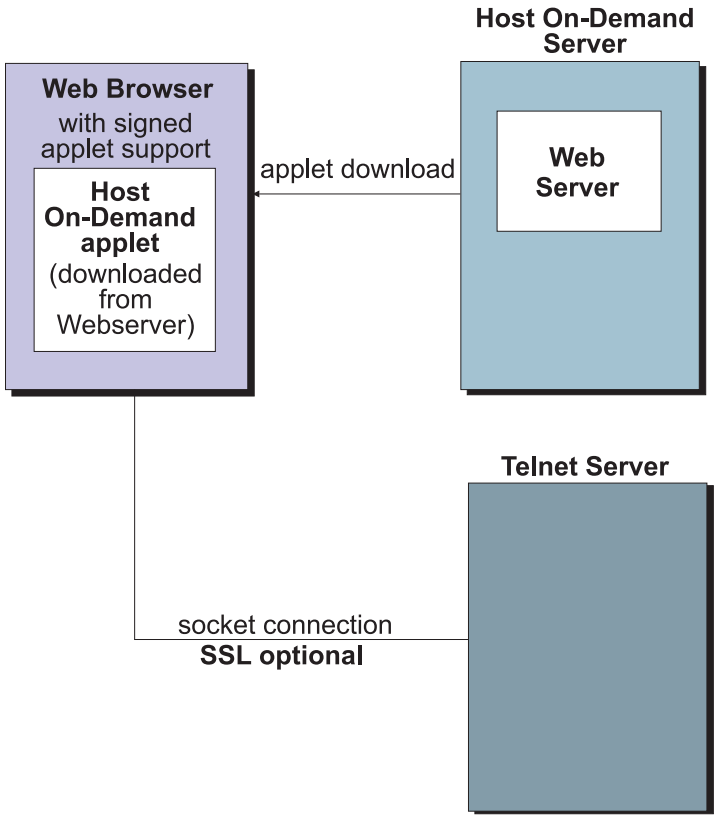
Benefits:

- Single server
- Session security if the Telnet server supports it

- Central administration

Figure 2

A client using a browser that supports signed applets can connect to any Telnet server.



Benefits:

- Signed-applet support allows access to multiple Telnet servers without the need for the Redirector
- Session security if the Telnet server supports it
- Central administration

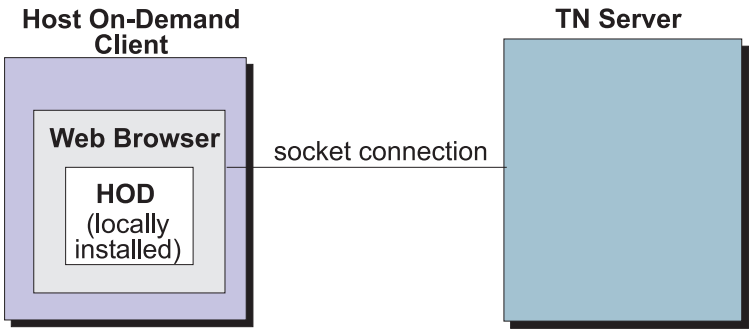
Locally-installed clients

Client workstations with Host On-Demand installed on them can:

- Connect directly to a Telnet server
- Connect indirectly to a Telnet server through a Host On-Demand server (Redirector)

Figure 3

A direct connection to a Telnet server can reduce response time; however, you cannot have connection security unless the Telnet server supports SSL. Clients can have connections to multiple Telnet servers.



When you install Host On-Demand on a client, you do not need a Host On-Demand Server unless you intend to use the Redirector which is part of a server installation.

Mixed environment - local and Download clients

If you have a network that includes both downloaded clients (for people in the office) and locally installed clients (for people working from home), you might want to use the Redirector for remote clients and SSL to ensure secure connections for all the clients. In that case, you would install a Host On-Demand Server and configure the Redirector to use secure connections.

Both office and remote users can run the Cached client as an alternative to the standard download or locally-installed client. This must be downloaded from a server only the first time you use it; thereafter, it is loaded from the local hard disk.

LDAP support

A Lightweight Directory Access Protocol (LDAP) server directory provides the ability to share user and group configuration information.

The following LDAP servers are supported for use with Host On-Demand:

IBM SecureWay Directory Server V2.1	NT and AIX
Netscape Directory Server V3.1 and V4.0	NT and AIX
IBM SecureWay Directory Server on OS/390 Version 2, Release 5, 6 and 7	OS/390

Installing LDAP support

1. Decide which LDAP Directory server you are going to use and if necessary install it. 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/`.
2. Install the Host On-Demand schema extension files.
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.
6. Migrate configuration information to the LDAP directory server (optional).

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.

Your LDAP administrator may have already installed these schema extensions for use by another IBM product. If so, skip these steps.

To install the Host On-Demand schema extensions on a Netscape LDAP Directory server:

1. Copy the following slapd files to the LDAP server:

```
Netscape.IBM.at
Netscape.IBM.oc
```

2. Stop the LDAP server.
3. Edit the `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 to your LDAP server:

```
V2.1.IBM.at
V2.1.IBM.oc
```

2. Stop the LDAP server.
3. Edit the `slapd.at.conf` file and add the following statement to the end of the file:

```
include /etc/V2.1.IBM.at
```

4. Edit the `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 LDAP support

The default operational mode for Host On-Demand is to use the private data store. 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. Before you switch your Host On-Demand server over to using the LDAP directory server, refer to implications of migrating to LDAP in the Host On-Demand online help.

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 this guide 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.

4. Click Apply.

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.

Database On-Demand overview

Database On-Demand is a Java applet that allows users to perform SQL requests to AS/400 databases through a JDBC driver. Database On-Demand is shipped with a JDBC driver for the AS/400. 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
- The ability to display on screen the results of the executable statements you build, or to save the results in various file formats
- The ability create dynamic queries, using the graphical interface, that can be executed or saved for later use

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

To configure users so they can access Database On-Demand, you must first either have groups and users defined or define them. 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.

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

National language support

Host On-Demand is provided in many 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 help.

All the translated versions are provided on the CDs and on the System/390 tapes. When you install Host On-Demand on Windows 95, Windows 98, Windows 2000, Windows NT 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. Arabic, Hebrew, Thai, and Hindi support is always installed on all operating systems.

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.

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.

Language	Language Suffix

Chinese (Simplified)	zh
Chinese (Traditional)	zh_TW
Czech	cs
Danish	da
Dutch	nl
English	en
Finnish	fi
French	fr
German	de
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	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	
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 Extended)	930	
Japan (Katakana Unicode Extended)	1390	3270 only
Japan (Katakana)	930	
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	
PRC (Simplified Chinese Extended)	1388	
ROC (Traditional Chinese Extended)	937	
ROC (Traditional Chinese Extended; Euro)	1371	
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	
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 supports only Latin-1, DBCS, BIDI, and Thai code pages.
- The new Simplified Chinese Code Page 1388 was replaced by the 935 code page.

VT code pages

Language	Code Page
British	1101
DEC Multinational Replacement Character Set	1100
Dutch	1102
Finnish	1103
French	1104
French Canadian	1020
German	1011
Italian	1012
Norwegian/Danish	1105
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
857	Latin 5
866	Cyrillic
869	Greek
912	ISO Latin 2 (8859_2)
915	ISO Cyrillic (8859_5)

920	ISO Latin 5 (8859_9)

Appendix A: 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 and Windows 2000
- Windows NT 4.0 with SP3 or later

The locally-installed client requires 155MB of disk space.

Installing Host On-Demand as a client

The Host On-Demand client can be installed on Windows 95, Windows 98, Windows 2000 or Windows NT. To install Host On-Demand on a Windows NT or 2000 workstation, you must be a member of the Administrators group.

1. Insert the CD and run `setup.exe lc` from the root 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 and 2000, the Service Manager is installed as a Service; on Windows 95 and Windows 98, it is added to the Startup folder.

Starting the client

To start Host On-Demand as a client, click Start > Programs > IBM Host On-Demand > Host On-Demand.

Removing the 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 InstallSheild does not remove the hostondemand directory you must remove it manually.

Appendix B: 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. You must also install JDK 1.1.8 or later.

Before installing the AIX server security files over an existing installation, you must remove all lib*.so files from the hostondemand/bin directory. There are different files for AIX V4.2 from those for V4.3.

These 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/local/server_directory
tar -xf /cdrom/tar/hod50AIX.tar
```

   The files extracted from hod50AIX.tar are:

   - hod50srv.AIX42.SSL.tar security files to be added to the server directory of an AIX 4.2 installation
   - hod50srv.AIX43.SSL.tar security files to be added to the server directory of an AIX 4.3 installation
   - GSK.AIX.tar installp image of the security code used by Host On-Demand

2. To add the extra files to the installation, untar the hod50srv.AIX43.SSL.tar file to the server directory. Enter the following commands:

```
cd /usr/local/server_directory
rm bin/lib*.so
tar -xf ../hod50srv.AIX43.SSL.tar (or hod50srv.AIX42.SSL.tar )
```

3. The GSK security library must also be installed. To extract the installp images, enter the following commands:

```
cd /usr/local/server_directory
tar -xf GSK.AIX.tar
cd images
```

4. From the /usr/local/images 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 GSKRF301 for AIX. Also highlight the line labeled GSKRU301 for AIX, 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.
   i. When installation finishes, exit smit and delete the files that you extracted from the GSK.AIX.tar file.

j. If you want to, delete the three files you extracted in step 1.

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 C: Configuring SSL capability for clients on AS/400

Before configuring clients for SSL on an AS/400, you must ensure that the AS/400 is SSL capable. Refer to the AS/400 documentation located at `http://publib.boulder.ibm.com/pubs/html/as400/v4r4/ic2924/info/java/rzahh/sslreq.htm` to determine if your AS/400 server is properly configured.

Configuring SSL for AS/400 clients

After ensuring the AS/400 is SSL capable, configure the Host On-Demand server for SSL. By default, AS/400 File Transfer and Database On-Demand support server certificates from the following companies:

- VeriSign, Inc
- Integrion Financial Network
- IBM World Registry
- Thawte Consulting
- RSA Data Security, Inc.

If you choose not to use a certificate from a trusted authority, you can build your own certificate, using the digital certificate manager (DCM). Create the certificate authority on the AS/400, then apply the certificate to the host servers.

Configuring the Host On-Demand server

- At a command prompt, change to your Host On-Demand `lib` directory (for example, `cd /usr/local/hostondemand/lib`), then run:

```
keyrng com.ibm.as400.access.KeyRing connect <systemname>:<port>
```

  The server port can be any of the host servers to which you have access. For example, 9476 is the default port for the AS/400 secure sign-on server.
- Type `toolbox` as a password.
- Select the number of the Certificate Authority (CA) certificate that you want to add to your AS/400. Be sure to add the CA certificate and not the site certificate. A message is issued stating that the certificate is being added to `com.ibm.as400.access.KeyRing.class` .

- Repeat step 3 for each certificate that you would like to add.

Download a separate certificate from each CA you would like to add to the `KeyRing.class` file.

- Copy the `KeyRing.class` file to `\hostondemand\hod\com\ibm\as400\access` directory.

Appendix D: Host access toolkit

The Host Access Toolkit consists of the Host Access Class Library, the Host Access Beans for Java, and Open Host Interface Objects (OHIO).

The Host Access Class Library provides a core set of classes and methods that allow the development of platform-independent applications that can access host information without the need for a graphical display. The library represents an object-oriented abstraction of a host connection that includes reading and writing the host presentation space, enumerating the fields in the presentation space, reading the operator information area (OIA) for status information, transferring files, and performing asynchronous notification of significant events.

The Host Access Beans provide emulator functions as a set of JavaBeans that can be used by developers to rapidly develop custom applications that deliver the specific functions they want.

The OHIO APIs set the standards for advanced interface to the TN3270 and TN5250 data. OHIO addresses the need for a common, advanced, client programming interface to the host datastream. Host On-Demand implements these standards in V5.

Complete information is available in these publications:

- *Host Access Class Library Reference*
- *Host Access Beans for Java Reference*
- *Open Host Interface Objects Reference*

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 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 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.

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 information 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.

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- AIX
- AS/400
- CICS
- IBM
- MVS
- OpenEdition
- OS/2
- OS/390
- OS/400
- S/390
- System/390

Lotus and Domino Go Webserver are trademarks of Lotus Development Corporation in the United States, or other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

Other company, product, and service names may be trademarks or service marks of others.