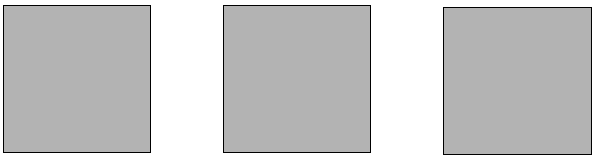

OC://WebConnect

Installation Guide

OPENCONNECT®
SYSTEMS

2711 LBJ Freeway, Dallas, TX 75234
Tel: 972/484-5200 • Fax: 972/484-6100

OpenConnect Systems® Incorporated continually updates its product publications. It is the user's responsibility to ensure that this edition is applicable and current before using this publication in conjunction with any OpenConnect Systems product. OpenConnect Systems makes no warranties with the respect to the contents of this publication and does not assume any liability arising out of the use of any product described in this publication.

Trademarks

The following trademarks are used in this guide:

- Product names associated with OpenConnect—Trademarks of OpenConnect Systems Incorporated.
- OpenConnect and OpenConnect Systems—Registered trademarks of OpenConnect Systems Incorporated.
- MS-DOS, Windows and Windows NT—Registered trademarks of Microsoft Corporation.
- UNIX—Registered trademarks of UNIX System Laboratories, Inc.

Document Revision History

Part Number IEN-WCT-IG

Release Date	Document Version	Change Description
Jan 06, 1997	.01	Software Version 2.6, International English
Sep 30, 1997	.02	Software Version 3.1, International English
Jan 22, 1998	.03	Software Version 3.2, International English

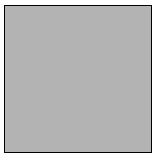
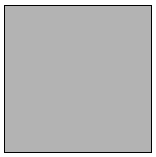
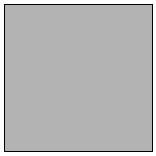

Table of Contents

Chapter 1

Overview

OpenConnect Systems Incorporated's OC://WebConnect™ combines in a single software package, the simplicity of Java-based web browsers, the security of RSA Data Security™, and OpenConnect Systems' internetworking technology. End users access information residing on IBM mainframe and midrange computers by downloading 3270/5250 Java Client Software, which is a Java applet. The Java applet is downloaded to the end user's web browser from an NT or UNIX OC://WebConnect server for Java. When executed, the applet opens a TCP/IP session with the server and makes a connection to an IBM mainframe or midrange computer. The Java applet displays the host session in a Java applet window and allows end users to access mainframe and midrange computers by using 3270, 5250, 3287, or VT terminal emulation.

This version of OC://WebConnect provides enhanced functionality, such as file transfer capabilities, support of Netscape's Secure Socket Layer protocol (SSL), and other features.

OC://WebConnect transfers files between a Java client and an SNA host application. You might want to transfer files between SNA hosts and Java clients to store large files on the host for use by host applications. Because SNA host files use different file formats than OC://WebConnect files and Java client files, use the appropriate options for converting files to the receiving host's file format during transfer. The format conversion allows the receiving host's applications to use the file.

Another feature of OC://WebConnect added to this release is the ability to configure OC://WebConnect to use the Secure Socket Layer (SSL) protocol. SSL allows a secure channel to be established between a client and server communicating over an untrusted network such as the Internet.

Note: Refer to Microsoft documentation for proper SNA server setup prior to configuring OC://WebConnect.

Chapter 2

UNIX

To install OC://WebConnect on your UNIX server:

1. Access the appropriate OC://WebConnect release file for the target system from:

UNIX diskette or tape

a. Insert the installation media into the tape drive.

b. Type tar xvf /device name/filename.

Caution: When you execute the tar command, any preexisting files in the tar working directory may be overwritten.

UNIX CD

a. Insert the compact disk into the CD drive.

b. Mount the CD ROM drive to your system.

To mount the CD ROM drive to your HP system:

1.) Make sure you have root privileges.

2.) Type the following command:

pfs_mount -x no_version /device name /file system name

Example:

pfs_mount -x no_version /dev/dsk/c0tzd0 /cdrom

Note: If your operating system is less the 10.10, download

the pfs mount program from HP.

c. Copy the installation file from the CD to your hard drive

Note: For CD installation, the installation file will have a .tar extension, not .tar.Z.

The following table shows operating systems and associated release files that OC://WebConnect currently supports:

Operating System	Release File
AIX	AX32DU.tar.Z AX32IU.tar.Z AX32DL.tar.Z AX32IL.tar.Z
HP-UX	HP32DU.tar.Z HP32IU.tar.Z HP32DL.tar.Z HP32IL.tar.Z
Solaris	SO32DU.tar.Z SO32IU.tar.Z SO32DL.tar.Z SO32IL.tar.Z
DEC	DX32DU.tar.Z DX32IU.tar.Z DX32DL.tar.Z DX32IL.tar.Z

The naming convention used is:

XXNNYZ*.tar.*Z

where ***XX*** is the Operating System, ***NN*** is the release number, ***Y*** is either Domestic (D) or International (I), and ***Z*** (L or U) indicates level of sessions supported.

2. Uncompress and extract the OC://WebConnect install script by entering the appropriate release filename in the following commands:

zcat filename.tar.Z|tar xvf -

or

tar xvf filename.tar

The tar command extracts the following files and stores them in your installation directory.

wc.tar

configure

installwc

InstalDE.txt (German)

ReadmeDE.txt

InstalEN.txt (English)

ReadmeEN.txt

InstalES.txt (Spanish)

ReadmeES.txt

InstalFR.txt (French)

ReadmeFR.txt

Note: Do not extract the wc.tar file.

3. Run the installwc install script by entering the following command:

   ./installwc

   Note: All log information from installwc is sent to both the screen and the wc.log log file. The log file is stored in the installation directory.

4. Press RETURN to install OC://WebConnect, or cancel by pressing any other key and RETURN.

5. Enter a full path of the directory in which you wish to install OC://WebConnect and press RETURN. Otherwise, press RETURN to accept the /usr/wc default path. The files are extracted.

6. Select a number for the language you want to use for server administration and press RETURN.

7. Press RETURN to configure the OC://WebConnect server. This will start up the configuration utility. See the next section for step by step configuration instructions.

8. To start OC://WebConnect, press RETURN.

9. To start OC://WebServer, press RETURN. Otherwise, enter n and press RETURN.

10. If you selected No in Step 9, you are asked if you want to configure the HTML files.

(See the OC://WebConnect User Guide and Reference Manual)

If you do not start the daemon, a message displays instructing you how to start the daemon manually later.

OC://WebConnect is now installed in your system.

Notes: After you start OC://WebConnect, you can access the server by running the wsd.exe and entering the following URL in your web browser:

http://[hostname]:[port number of web server].

The following example uses the default setup options:

http://host1.oc.com:2080

If the server does not start after you install it, use the configuration utility to configure the correct port and reconfigure your server.

To Configure OC://WebConnect for UNIX using configuration utility:

To configure OC://WebConnect for UNIX using the configuration utility:

1. Execute the configure script by entering the following command from the OC:// WebConnect directory (default is **wc**):

./configure

2. The following menu will be displayed.

1) Configure OC://WebConnect Ports
2) Configure Default 3270 Session
3) Configure Default 5250 Session
4) Configure Default VT220 Session
5) Configure Default 3287 Session
6) Configure License Key Information
7) Configure Default Administration Language
8) Configure OC://WebServer HTTP Port
9) Configure OC://WebConnect SSL

0) Exit

3. Press RETURN each time the main menu is displayed and you will be auto-sequenced through each of the menu items. Or if you wish to go directly to configure a specific item, enter the number of your selection and press RETURN. For the initial configuration of the OC://WebConnect installation, you should use the auto-sequence feature and configure all listed items. Each configuration item is discussed in the section following this one.

4. After completing each server configuration option the OC://Webconnect HTML files are automatically updated. This is relevant for anyone using the OC://Webconnect provided HTML files either directly or as a model for customization. All files in the OC://Webconnect html directory will be scanned for host name, port parameters, and server language. They are then updated with the current settings. Any HTML files stored in another directory will not be updated.

   Failure to update HTML files may make it difficult to access and configure OC:// Webconnect via a browser, start an emulation session, or retrieve server status information.

5. If the RETURN key is pressed each time the main menu is displayed, the configuration will auto-sequence through each of the menu items.

6. Choose menu item **0)Exit** when configuration has been completed.

7. For the changes to take affect **Restart** the OC://Webconnect servers after exiting the configuration utility.

OC://WebConnect Configuration Options

1) Configure OC://WebConnect Ports

Each OC://WebConnect service can listen to incoming requests and send data back on one or all of the network interfaces installed on a UNIX platform. The configuration utility lists all of the IP addresses for the network interfaces detected. The default **0.0.0.0** causes OC://WebConnect servers to respond to requests from all installed network interfaces. Specify another IP address to limit OC://WebConnect to one network interface.

The OC://WebConnect server uses up to four ports during operation. You may choose to use the defaults, shown below, by pressing RETURN at each prompt, or you may

choose to enter a port number greater than **0** or less than **65,535**. Root privileges are required to use a port less that **1024**. A port number of **0** disables a port.

In a TCP/IP communication, a port is a number assigned to an application program running in a destination computer. The number is used to link the incoming data to the correct application. There are many de facto standard port addresses. For example, port 80 is used for HTTP (Web) traffic. In the case of OC://WebConnect, there are four possible ports with only one port required:

IP Address & Default Port Number	**Service**	**Description**
0.0.0.0:3270	Java Server	Listening port for non-SSL java emulation clients. Required.
0.0.0.0:3443	Secure Java Server	Listening port for java emulation clients using administration clients. Optional if not using SSL.
0.0.0.0:4270	Java Administration	Listening port for use by CGIbin interface to obtain configuration parameters, to launch applets, and for retrieving server status information. Optional if using static html and not reporting server Status information.
0.0.0.0:2080	HTTP Server	Serves HTML traffic for HTML configuration parameters to launch applets and for retrieving server status information. Optional if using a third party HTTP server.

After entering the service ports you are given an opportunity to update HTML files. This is relevant if you are using the OpenConnect-provided HTML files either directly or as a model to create your own. If you enter **yes**, all files in the html directory will be scanned for port parameters, and updated with the current settings.

2) Configure Default 3270 Session

This selection allows the configuration of the Domain Name Server (DNS) host name or IP address and TCP port address of a TN3270 server, TN3270E, or gateway for mainframe access. This information is used to create the default 3270 session configuration. Other default session settings and additional 3270 sessions may be

configured later using the OC://WebConnect Quick Connection or OC://WebConnect GUI Configurator or OC://WebConnect HTML Config Utilities.

3) Configure Default 5250 Session

This selection allows the configuration of the Domain Name Server (DNS) host name or IP address and TCP port address of a TN5250 server or gateway for midrange emulation access. This information is used to create the default 5250 session configuration. Other default session settings and additional 3287 sessions may be configured later using the OC://WebConnect Quick Connection or OC://WebConnect GUI Configurator or OC://WebConnect HTML Config Utilities.

4) Configure Default VT220 Session

This selection allows you to configure the DNS host name or IP address and TCP port address of a TELNET server or gateway for ASCII terminal emulation access. This information is used to create the default VT220 session configuration.

5) Configure Default 3287 Session

This selection allows you to configure the DNS host name or IP address and TCP port address of a TN3287 or TN3270E server or gateway for mainframe printer emulation access. This information is used to create the default 3287 Print session configuration. Other default session settings and additional 5250 sessions may be configured later using the OC://WebConnect Quick Connection or OC://WebConnect GUI Configurator or OC://WebConnect HTML Config Utilities.

6) Configure License Key Information

OC://WebConnect comes prepackaged with a license key to enable the server for a specific number of concurrent sessions and key expiration. Press RETURN to install the default key. If a special or replacement key has been provided, enter it at the prompt and press RETURN. The number of concurrent sessions and expiration date for the key configured can be seen when the OC://WebConnect servers are started on the OC://WebConnect STATUS Page, log file, or trace file.

7) Configure Default Administration Language

OC://WebConnect cab be configured to one of four possible server languages;

- English
- French
- German
- Spanish.

When the server language is changed, the HTML files provided with OC://WebConnect automatically are updated including any previous configured server host names or ports.

8) Configure OC://WebServer HTTP Port

Each OC://WebConnect service can listen to incoming requests and send data back on one or all of the network interfaces installed on a UNIX platform. The configuration utility lists all of the IP addresses for the network interfaces detected. The default **0.0.0.0** causes OC://WebConnect servers to respond to requests from all installed network interfaces. Specify another IP address to limit OC://WebConnect to one network interface.

To use the OC://WebConnect HTTP Web server, enter a TCP port number for the HTTP service. This is the port number which is used when accessing OC://WebConnect via a browser.

Example: http://host1.oc.com:2080

The default OC://WebConnect HTTP Web server port is **2080**. Many HTTP Web servers us port **80** because most browsers default to port **80**. Therefore, the browser user has only to enter the Web server host name and not a port.

Example: http://host1.oc.com

A port number of **0** disables the OC://WebConnect HTTP Web Server.

9) Configure OC://WebConnect SSL

To use OC://WebConnect SSL authentication and encryption features, either a key pair and certificate or a “generate a certificate request” must be generated.

If a key pair and certificate is generated, answer YES to enable SSL. At this point, SSL is fully operational when the OC://WebConnect server is started.

If the “generate a certificate request” is chosen, the request must be submitted to a Certificate Authority (CA). SSL cannot be used until the certificate has been received and the CA manually installed in the OC://WebConnect security directory and the configure utility is rerun to enable SSL.

When executing the configure utility, answer NO when asked to generate a new key pair, then answer YES when asked to enable SSL.

See the section below, “Key Pair & Certificate Generation for UNIX,” for step by step instructions.

0) Exit

This selection will exit the configuration utility.

After completing configuration you may restart OC://WebConnect by entering the following command:

./wcd

If you are using the OpenConnect-provided web server, enter the following command:

./wsd

Note: The configuration utility for all platforms needs to be run with all OC://WebConnect services stopped. Configuration changes will not take effect until the services are restarted.

Key Pair and Certificate Generation for UNIX (ocssladm)

OC://WebConnect must be setup with a key pair and certificate before the SSL features can be used. Specific information is required about the length of key and company to generate the RSA key pair and certificate or a certificate request for the OC://WebConnec server. Each panel presents detailed information concerning a particular question, followed by the actual question.

For the optimum performance/convenience vs. security trade-off, the default settings are recommended.

The following questions are asked:

1. Choose a value between 512 and 2048 bits for the RSA modulus length? [1024]

If 512 bit modulus is chosen, skip the next question (Step 2) and proceed to directly to Step 3.

2. Generate server-wide key exchange key pair (yes/no)? [yes]

This question is only relevant if you intend to configure exportable (40-bit) ciphers for this installation. If "yes" is chosen, a 512-bit key is used for these ciphers, rather than waiting until session startup. This improves session connect times and helps prevent the server from becoming bogged down computing keys on heavily loaded servers.

3. Store password on server system (yes/no)? [yes]

A password is used to secure the server's private key. The system administrator needs to type in this password each time OC://WebConnect is started, making unattended restarts impossible, unless the password is stored on the server system. Thus, the administrator must choose between the convenience of unattended restart or the additional security.

Regardless of whether the password is stored on the server, the OC://WebConnect security directory must be access-protected to prevent potential attackers from compromising the server. With this perspective, the slight reduction in security from storing the password on the server may be a reasonable trade-off for the increased convenience of having an automatic restart capability.

4. The password may be any combination of displayable characters, including spaces, up to 100 characters in length.
Shall I turn off echo while you enter the password (yes/no)? [yes]
Enter the password at this time:

After entering the password, the RSA key pair is generated. This may take anywhere from a couple of seconds for shorter keys, to over an hour for extremely long keys. A 1024-bit key should normally complete within a minute or two depending on the system. A second key, 512 bits, is generated if a server-wide key exchange key pair is generated.

5. Specific site information is needed to generate a certificate request. This information pertains to the name and location of the server.

- DNS name of server: [hostname]
- Company name or organization:
- Organizational unit, division, etc. (this field is optional):
- City:
- State:
- Country (use ISO Country Code -- do not spell out): [US]

The data entered in these fields comprise the X.500 “distinguished name” of the subject listed in the body of the certificate. If a built-in certificate generator or a private CA is used, then what is entered in these fields is somewhat arbitrary, but is intended to uniquely identify the holder of the certificate. If a third-party CA is used, it is important that the name be unique, and all fields accurate. The “State” should be spelled out.

6. Shall I generate the Certificate, or shall I generate a certificate Request instead? Generate certificate (yes/no)? [yes]

Choose YES to allow the built-in certificate generator to generate a certificate, or NO to generate a PKCS #10 certificate request to be submitted to a third-party or private CA.

The default method of server authentication used by OC://WebConnect SSL clients is to compare the computed fingerprint of the server’s certificate to the fingerprint received as an applet startup parameter from the web server. Therefore, it is not necessary to use a CA to generate the OC://WebConnect server certificate. The setup for server authentication is handled automatically if the default method is chosen and OC://WebConnect-provided CGIbin for applet startup is used.

Alternatively, if NO is chosen only the certificate request is generated. The request is submitted to a CA. Manually install the certificate into the security directory and rerun configure. With a CA-generated certificate, it may be desirable for your clients to authenticate the server using the CA’s certificate rather than the server’s. This approach can provide a more centralized security model, but is more cumbersome to implement.

If a CA is chosen instead of the built-in certificate generator, skip to question #8.

7. Term of validity for certificate in hours: [8760 (1 yr)]

The certificate is generated with a validation period starting at the time the certificate is generated. The period of time entered here determines the expiration date of the certificate.

At this point, the certificate is generated without asking question #8.

8. I’ll need some more information concerning the person responsible for receiving the certificate from the CA.

- E-mail address:
- Phone number:

Fill out these fields and press RETURN. Third party and private CAs use the phone number or e-mail address in the request to contact the person responsible,

if additional information is needed, or if problems arise. The completed certificate is typically delivered via e-mail, in base 64 encoding, to the e-mail address provided in the request.

The server certificate must be stored with the CA certificate(s), all base 64-encoded, in a file named **cert.txt**, with server certificate first to root CA certificate last order, in the security sub-directory of the OC://WebConnect home directory. After the certificate has been installed, rerun the “configure” utility to enable SSL.

To make OC://WebConnect clients validate to the CA rather than the server certificate, HTML has to be created for applet startup with the following applet parameter:

<param name="certfpca" value="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx">

where the x’s represent the fingerprint (MD5 hash) of the CA certificate in hexadecimal.

Chapter 3

Windows NT Installation

To install OC://WebConnect on your Windows NT Server:

1. Download the OC://WebConnect release file for Windows NT, or insert the CD into your CDROM drive.

2. If you are installing from a CD, access the CDROM drive and double-click on the OC://WebConnect installation program (NT32xx.exe). If you downloaded the release file, double-click the installation program you downloaded (NT32xx.exe).

   The following table shows the release files that OC://WebConnect currently supports depending upon your license:

   NT32DU.exe

   NT32IU.exe

   NT32DL.exe

   NT32IL.exe

   The naming convention used is:

   ***XXNNYZ*.exe**

   where ***XX*** is the Operating System, ***NN*** is the release number, ***Y*** is either Domestic (D) or International (I), and ***Z*** (L or U) indicates level of sessions supported.

3. Select Yes to install. The Custom Path Selection window displays.

4. Type the drive and directory in which OC://WebConnect files are to be installed and click Next. The default is C:\WC. The Java Server Information window displays.

   Note: If you are installing over an existing OC://WebConnect server, such as in the same directory, you will be prompted to continue the installation. You then will be notified that a previous version of OC://WebConnect already is installed

and have the option to replace the registry entry. Click Yes to continue, and click No to abort.

5. If you want to allow java clients to connect to the OC://WebConnect server without using SSL, enter the desired port number for the Java Server or accept the default (3270), and click Next. Enter 0 to disable this service.

6. If you are installing SSL, enter the desired port number for the Secure Java Service, or accept the default (3443), and click Next. Enter 0 to disable this service.

7. OC://WebConnect provides a Java Administration Server for a CGI-BIN to obtain startup parameters to launch java applets, and to retrieve session status. If you will be using this service, enter the desired port number, or accept the default (4270), and click Next. Enter 0 to disable this service.

8. If you plan to use OC://WebConnect for mainframe access using TN3270, enter the host name and TCP port address of a TN3270 server or gateway. This information is used to create the default 3270 session settings. You may configure additional TN3270 sessions later, to the same, or any other TN3270 server, using the OC://WebConnect GUI Configurator or OC:// WebConnect HTML Config Utilites.

9. If you plan to use OC://WebConnect for mainframe access using the Microsoft SNA Server, enter the name of a LU or LU pool. This information is used to create the default 3270 RUI session settings. You may configure additional 3270 RUI sessions later, using the OC:// WebConnect GUI Configurator or OC://WebConnect HTML Config Utilites.

10. If you plan to use OC://WebConnect for midrange access using TN5250, enter the host name and TCP port address of a TN5250 server or gateway. This information is used to create the default 5250 session settings. You may configure additional TN5250 sessions later, to the same, or any other TN5250 server, using the OC://WebConnect GUI Configurator or OC:// WebConnect HTML Config Utilites.

11. .If you plan to use OC://WebConnect for ASCII terminal emulation, enter the host name and TCP port address of a TELNET server or gateway. This information is used to create the default VT220 session settings. You may configure additional VT220 sessions later, to the same, or any other TELNET server, using the OC://WebConnect GUI Configurator or OC:// WebConnect HTML Config Utilites.

12. If you plan to use OC://WebConnect for 3287 printing, enter the host name and TCP port address of a TN3287 or TN3270E server or gateway.

This information is used to create the default 3287 session settings. You may configure additional 3287 sessions later, to the same, or any other TN server, using the OC://WebConnect GUI Configurator or OC:// WebConnect HTML Config Utilites.

13. OC://WebConnect comes prepackaged with a license key to enable the server for the correct user count. Normally, you will just click Next to install this key. If you have a special or replacement key, enter the license key number. Click Next.

14. Select the default administration language and click Next.

15. OC://WebConnect provides a web server you can use for launching the OC://WebConnect java applets and performing administrative functions. If you plan to use this server, enter the desired port number, or accept the default (2080), and click Next.

16. If you are installing SSL, click the YES button when it asks if you want to generate a key pair and certificate. You will then be presented with a sequence of dialog boxes to get the necessary information to generate the RSA key pair and certificate, or certificate request. This procedure is identical to the procedure for SSL setup on UNIX, with the exception that you click the Yes or No button, or Next, instead of typing yes or no and RETURN.

See "Key Pair & Certificate Generation for UNIX (ocssladm)" above for step by step instructions.

If you choose to generate a certificate, you will be offered the option to enable or disable SSL for the OC://WebConnect server after the certificate has been generated. Click Yes to enable SSL.

If you choose to generate a certificate request instead, you will need to submit the request to your CA. You will not be able to use SSL until you have received the certificate from the CA, manually installed it in the OC://WebConnect security directory and rerun the configuration utility to enable SSL. When you rerun "configure," make sure and answer NO when it asks if you want to generate a new key pair and certificate. This will take you directly to the prompt to enable SSL for the server.

17. After completing OC://WebConnect configuration, you will be given an opportunity to update HTML files. This is relevant if you will be using the OpenConnect-provided HTML files either directly or as a model to create your own. If you enter yes, all files in the html directory will be scanned for port parameters, and updated with the current settings.

18. Click the checkbox to view the README file.

19. Click Finish to complete setup.

To Configure OC://WebConnect for NT using the Configuration Utility:

To start the OC://WebConnect Configuration Utility:

1. Select **Start** menu on the Windows NT taskbar.

2. Select **OC://WebConnect rel#**

3. Select **OC://WebConnect Configuration Utility**.

After completing each server configuration option, the OC://WebConnect HTML files are automatically updated. This is relevant for anyone using the OC:// WebConnect-provided HTML files whether directly or as a model for customization. All files in the OC://WebConnect html directory are scanned for host name, port parameters, and server language. Then, they are updated with the current settings. Any HTML files stored in another directory are not updated.

4. When current configuration information is displayed, press RETURN to accept the current information. Change the information that needs to be modified. See each configuration item discussed for UNIX (Chapter 2).

5. For the changes to take effect, restart the OC://WebConnect servers after exiting the configuration utility.

To Start OC://WebConnect for NT:

After the installation is complete, start OC://WebConnect by selecting Settings from the Start button on the Windows taskbar.

1. From Settings, select Control Panel.
2. Double-click Services in Control Panel.
3. Scroll to OC://WebConnect Server XX in the list, or select another server if you are not using the OC://WebConnect server. Select OC://WebConnect Server XX and click the Start button.

   Note: If the service did not start, you will receive an error message from service control that the service cannot be started. Check the Event Viewer under Application Log to review any error messages for OC://WebConnect.
4. Scroll to OC://WebServer XX in the list, or select another server if you are not using the OC://WebServer. Select OC://WebConnect Server XX and click the Start button.
5. Access the OC://WebConnect server by entering the following URL in your web browser:

   http://[NT server name]:[port number of web server]

   The following example uses the default setup options:

   http://server1.oc.com:2080

   Note: Windows NT 3.51 users can open the Services window by selecting Main, Control Panel, Services.

To Install OCS Terminal Font (True Type Font)

1. Install the OCS terminal font on your PC where the browser is installed. Run the ocs_font.exe from the samples directory.

2. Modify the font properties in the browser and apply the following changes.

   #monospaced.0=Courier New,ANSI_CHARSET

   monospaced.0=OCS Terminal,ANSI_CHARSET

3. Start your JDK 1.1-supported browser to use the new font.

   Note: All the applets will use the new font, and is NOT limited to OC://Webconnect applets.

Chapter
4

Hardware Requirements

MVS and VS Systems

For MVS and VS systems, you are required to have a TN3270 server to connect the mainframe and OC://WebConnect. Some servers include: OC Server II (OCSII), IBM MVS TCP/IP, IBM AIX SNA Server, Microsoft SNA Server. For AS/400 systems, you are required to have a TN5250 server, such as OpenConnect's OC Server II, to connect the mainframe and OC://WebConnect.

Comment Card

Your Comments Please . . .

Your comments can help us improve the usefulness of this document. Possible comment topics can include:

- Clarity
- Accuracy
- Organization
- Figures
- Tables
- Terminology
- Examples
- Questions

Page	Comment

Note: Attach additional comments, if needed.

Reader's Name: _____

Title: _____

Company: _____

Address: _____

City, State, Zip: _____

Telephone: _____

Send Comment Card to:

Documentation Manager
OpenConnect Systems
2711 LBJ Freeway, Suite 800
Dallas, Texas 75234
Fax 972/888-0688