OC://WebConnect
Version 3.5

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 are trademarks of OpenConnect Systems Incorporated.
- OpenConnect and OpenConnect Systems are registered trademarks of OpenConnect Systems Incorporated.
- MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.
- UNIX is a registered trademark of UNIX System Laboratories, Inc.

Document Revision History

Part Number IEN-WCT-IG

Release Date	Document Version	Change Description
July 1998	.04	Software Version 3.5, International English
January 1998	.03	Software Version 3.2, International English
September 1997	.02	Software Version 3.1, International English
January 1997	.01	Software Version 2.6, International English

Contents

Chapter 1

Overview

The OpenConnect Systems Incorporated OC://WebConnect™ product combines in a single software package the simplicity of Java-based Web browsers, the security of RSA Data Security™, and the OpenConnect Systems internetworking technology. End users access information residing on IBM mainframe and midrange computers by downloading 3270/5250 Java client software, 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 connects 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.

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

Chapter 1

UNIX

Installing OC://WebConnect

To install OC://WebConnect on your UNIX server, follow these steps:

1. Access the appropriate OC://WebConnect release file for the target system from diskette, tape or CD:

UNIX Diskette or Tape

a. Insert the diskette or tape into the device drive.

b. Type the following command:

```
tar xvf/device name/filename
```

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

UNIX CD

a. Insert the compact disk into the CD drive.

b. Mount the CD ROM drive to your system.

After ensuring you have root privileges, 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 lists 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 AX32DE.tar.Z AX32IE.tar.Z
HP-UX	HP32DU.tar.Z HP32IU.tar.Z HP32DL.tar.Z HP32IL.tar.Z HP32DE.tar.Z HP32IE.tar.Z
Solaris	SO32DU.tar.Z SO32IU.tar.Z SO32DL.tar.Z SO32IL.tar.Z SO32DE.tar.Z SO32IE.tar.Z
DEC	DX32DU.tar.Z DX32IU.tar.Z DX32DL.tar.Z DX32IL.tar.Z DX32DE.tar.Z DX32IE.tar.Z

The naming convention is *xxnnyz***.tar.Z,** where *xx* is the operating system, *nn* is the release number, *y* is D for domestic or I for international, and *z* indicates level support: L for limited sessions, U for unlimited sessions, and E for 8-user evaluation copy with an expiration date.

2. Uncompress and extract the OC://WebConnect installation script by entering the appropriate release file name in one of 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** installation script by typing 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. Type the full path of the directory in which you wish to install OC://WebConnect and press RETURN.

   -or-

   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. The following message displays:

   Would you like to configure the WebConnect daemons now (yes/no)? [yes]

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

Note: You can later run the configuration utility stand-alone. Refer to the *OC://WebConnect User's Guide and Reference*.

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

9. To start OC://WebServer, press RETURN. Otherwise, type **n** (no) and press RETURN.

   If you selected No in Step 9, you are asked if you want to configure the HTML files. See the *OC://WebConnect User's Guide and Reference*.

   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 **wsd.exe** and typing the following URL in your Web browser:

   http://*hostname*:*WebServerPort*

   The following example uses the default setup options:

   http://host1.oc.com:2080

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

Configuring OC://WebConnect for UNIX

Note: Ensure that all OC://WebConnect services are stopped before starting the configuration utility for all platforms. Configuration changes take effect when the services are restarted.

To configure OC://WebConnect for UNIX using the configuration utility, follow these steps:

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

```
./configure
```

The following menu is 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
```

2. Press RETURN each time the main menu is displayed and you are automatically stepped through each menu item.

-or-

To go directly to configure a specific item, type the number of your selection and press RETURN.

Note: For the initial configuration of the OC://WebConnect installation, use the auto-stepping feature to ensure that you configure all listed items. Each configuration item is discussed in the following section.

After you complete 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 are scanned for host name, port parameters, and server language. They are then updated with the current settings. Any HTML files stored in another directory are not updated.

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

3. Choose menu item **0)Exit** when configuration is complete.

4. For the changes to take effect, 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 network interfaces installed on a UNIX platform. The configuration utility lists all 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 can choose to use the defaults, shown below, by pressing RETURN at each prompt.

-or-

You can enter a port number greater than **0** and less than **65,535**. Root privileges are required to use a port less than **1024**. A port number of **0** disables a port.

In TCP/IP communication, a port number is 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. OC://WebConnect allows up to four ports, one of which is 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 to retrieve server status information. *Optional* if using static html and not reporting server status information.
0.0.0.0:2080	HTTP Server	Listening port for HTML traffic for HTML configuration parameters to launch applets and for retrieving server status information. *Optional* if using a third-party HTTP server.
0.0.0.0:2443	HTTPS Server	SSL-protected service for operating the HTML-based configurator and for invoking **cgiinfo** for launching applets. A third-party Web server can be used to perform the latter function.

After entering the service ports, you are given an opportunity to update HTML files. This is relevant if you use the OpenConnect-provided HTML files either directly or as a model to create your own. If you type **yes**, all files in the **html** directory are 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 can be configured later using the OC://WebConnect GUI Configurator or the OC://WebConnect HTML configuration 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 can be configured later using the OC://WebConnect GUI Configurator or the OC://WebConnect HTML configuration 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 can be configured later using the OC://WebConnect GUI Configurator or OC://WebConnect HTML configuration 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 can be configured to one of four 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 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 uss 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.

To operate the OC://WebConnect Web server using SSL, enter a TCP port number for the HTTPS service. This port number is used when accessing OC://WebConnect via a browser with the HTTPS protocol.

Example: Example:https://SSL-host1.oc.com:2080

The default OC://WebConnect HTTPS port is 2443. Many HTTPS Web servers use port 443 because most browsers default to port 443. Therefore, the browser user has only to enter the secure Web server host name without specifying a port.

Example: Example:https://SSL-host1.oc.com

A port number of 0 disables the OC://WebConnect HTTPS Service.

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 **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 and Certificate Generation for UNIX," for step-by-step instructions.

0) Exit

This selection exits the configuration utility.

After completing configuration, restart OC://WebConnect by typing the following command:

```
./wcd
```

If you are using the OC://WebServer, type the following command:

```
./wsd
```

Key Pair and Certificate Generation for UNIX (ocssladm)

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

For the optimal performance/convenience versus 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 directly to Step 3.

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

   This question is relevant only 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 types this password each time OC://WebConnect starts, 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 might be a reasonable trade-off for the increased convenience of having an automatic restart capability.

   The password can be any combination of displayable characters, including spaces, up to 100 characters in length.

4. Shall I turn off echo while you enter the password (yes/no)? [yes]

5. Enter the password at this time:

   After you type the password, the RSA key pair is generated. This can take anywhere from a few seconds for shorter keys to over an hour for extremely long keys. A 1024-bit key normally completes 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.

6. 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.

7. 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 might 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 10.

8. 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 10.

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

- E-mail address:
- Phone number:

Type the requested information 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*">

The *x*'s represent the fingerprint (MD5 hash) of the CA certificate in hexadecimal.

Chapter 2

Windows NT Installation

Installing OC://WebConnect on a Windows NT Server

To install OC://WebConnect on your Windows NT server, follow these steps:

1. Download the OC://WebConnect release file for Windows NT.

-or-

Insert the CD into the CD-ROM drive.

2. If installing from a CD, access the CD-ROM drive and double-click the OC://WebConnect installation program (NT32xx.exe).

-or-

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 on your license:

NT32DU.exe

NT32IU.exe

NT32DL.exe

NT32IL.exe

NT32DE.exe

NT32IE.exe

The naming convention is *xxnnyz*.**tar.*Z*,** where *xx* is the operating system, *nn* is the release number, *y* is D for domestic or I for international, and *z* indicates level support: L for limited sessions, U for unlimited sessions, and E for 8-user evaluation copy with an expiration date.

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 given the option to replace the registry entry. Click **Yes** to continue **No** to abort.

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

6. If you are installing SSL, type the desired port number for the Secure Java Service or accept the default (3443) and click Next. Type 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, type the desired port number or accept the default (4270) and click **Next**. Type 0 to disable this service.

8. If you plan to use OC://WebConnect for mainframe access using TN3270, type 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 can later configure additional TN3270 sessions to the same or any other TN3270 server, using the OC://WebConnect GUI Configurator or OC://WebConnect HTML configuration utilities.

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

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 can later configure additional TN5250 sessions to the same or any other

TN5250 server, using the OC://WebConnect GUI Configurator or OC://WebConnect HTML configuration utilities.

11. If you plan to use OC://WebConnect for ASCII terminal emulation, type 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 can later configure additional VT220 sessions to the same or any other TELNET server using the OC://WebConnect GUI Configurator or OC://WebConnect HTML configuration utilities.

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 can later configure additional 3287 sessions to the same or any other TN server, using the OC://WebConnect GUI Configurator or OC://WebConnect HTML configuration utilities.

13. 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.

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)” on page 13 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**, answer NO when asked if you want to generate a new key pair and certificate. This takes 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.

Configuring OC://WebConnect for NT

To configure OC://WebConnect for NTusing the configuration utility, perform these steps:

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.

Installing OC://WebPrint

To install OC://WebPrint, follow these steps:

1. From the main OC://WebConnect window, select OC://WebPrint on the left side of the window. The Install WebPrint for Java window displays.
2. Click OK to download OCWebPrint.exe, which is a self-extracting, zipped executable file.
3. When requested, select the download path on your system. OCWebPrint.exe is written to the path selected.
4. Shut down your browser.
5. Run OCWebPrint.exe and follow the prompts to install OC://WebPrint.
6. Restart your browser.

WebPrint is now available for use with all OC://WebConnect screen print functions.

Starting OC://WebConnect for NT

After the installation is complete, follow these steps to start OC://WebConnect for NT:

start OC://WebConnect by selecting Settings from the Start button on the Windows taskbar.

1. From the Windows taskbar, click **Start**>**Settings**>**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 **Start**.

   Note: If the service does not start, you receive an error message from service control that the service cannot be started. Check the Event Viewer under Application Log and 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 typing the following URL in your web browser:

   http://*NTServerName*:*WebServerPort*

   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**.

Installing OCS Terminal Font (True Type Font)

To install OCS terminal font, follow these steps:

1. Install the OCS terminal font on your PC where the browser is installed. Run **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 applets will use the new font. The change is *not* limited to OC://Webconnect applets.

Chapter 3

Hardware Requirements

MVS and VS Systems

MVS and VS systems must have a TN3270 server to connect the mainframe and OC://WebConnect. Some TN3270 servers are OC://WebConnect SNA Access Server (formerly called OCSII), IBM MVS TCP/IP, IBM AIX SNA Server, and Microsoft SNA Server.

AS/400 Systems

AS/400 systems must have a TN5250 server, such as OC://WebConnect SNA Access Server, 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