OC://WebConnect Pro
Version 3.5

User Guide and Reference

OPENCONNECT®
SYSTEMS

2711 LBJ Freeway, Suite 800, Dallas TX 75234
Phone: (972) 454-5200 • Fax: (972) 888-0688

Part Number IEN-WCT-UM

OpenConnect Systems® Incorporated continually updates its product publications. It is the user 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 respect to the content of this publication and does not assume any liability arising from the use of any product described in this publication.

Trademarks

Document Revision History

Part Number IEN-WCT-UM

Release Date	Document Version	Change Description
August 1998		Software Version 3.5

Contents

Chapter 1: Introduction and Overview

Introduction to OC://WebConnect Pro

OC://WebConnect Pro provides reliable, secure, and scalable host access using a Java™-enabled Web browser. To deliver traditional host-access emulation features over an intranet or the Internet, OC://WebConnect Pro combines the strengths of traditional client/server technology with the network access and ease of use of popular browsers and Java technology.

Secure host access over an intranet or the Internet is provided with an OC://WebConnect Pro Java client on a Java-enabled browser and the OC://WebConnect Pro server on UNIX or NT, all secured by Secure Socket Layer (SSL) authentication and encryption or RSA Data Security™ encryption.

OC://WebConnect Pro Architectural Overview

OC://WebConnect Pro uses a three-tier architecture to provide 3270, 3287, 5250, and VT emulation sessions via Web access. As shown in Figure 1, OC://WebConnect Pro has these components:

- OC://WebConnect Pro Java client applets launched from a Java-enabled Web browser
- The OC://WebConnect Pro Web emulation server
- Any TN or Telnet server

The OC://WebConnect Pro product includes the emulation server and Java client applets for 3270, 3287, 5250, and VT. The Java-enabled Web browser and TN or Telnet server must be purchased separately. The TN server can be purchased from OCS.

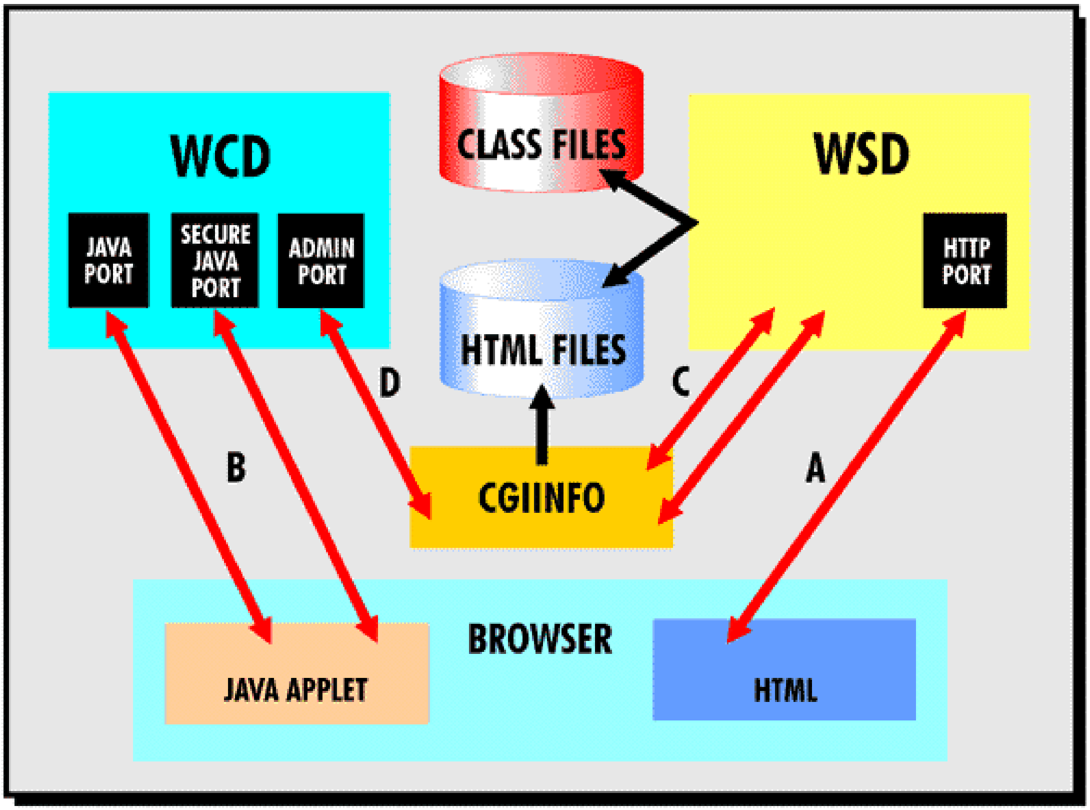


Figure 1: OC://WebConnect Pro Three-Tier Model

Establishing a Host Emulation Session from a Web Browser

OC://WebConnect Pro provides persistent emulation-session connectivity through the Java emulation client applets. The connection develops in this sequence:

1. The Java-enabled browser connects to the OC://WebConnect Pro HTTP server or third-party HTTP server and downloads the Java emulation client applet as needed.
2. The client applet creates and maintains an emulation client user interface (see connection A in Figure 1).
3. The applet opens a persistent socket connection with the OC://WebConnect Pro emulation server (see connection B in Figure 1), which then completes the three-tier model by opening a direct socket connection with the configured TN server.

The result is a direct logical session connection from the Web browser client to the host through the TN or Telnet server.

Full-Featured Emulation

OC://WebConnect Pro provides all the features of traditional emulation clients with centralized management of a server. Java applets are included for 3270, 3287 print, 5250, and VT emulation. Other major features include 3270E protocol support, print screen, copy/paste, hot spots, IND$FILE transfer, and administrator or end user mapping of user interface options such as keyboard and color emulation. Administrative features include server session status, kill session, and RTM (Response Time Monitor).

☞

More Information

For more information about emulation features and creating, deleting, and modifying session configurations, refer to the following chapters:

- *Chapter 6: Configuring 3270 Sessions*
- *Chapter 7: Configuring 5250 Sessions*
- *Chapter 8: Configuring 3287 Print Sessions*
- *Chapter 9: Configuring VT Sessions*

Installation, Configuration, and Maintenance

Installation and Setup

The OC://WebConnect Pro product is designed for easy installation and maintenance. To deploy OC://WebConnect Pro, an administrator performs a one-time installation of the full OC://WebConnect Pro product on a UNIX or NT server and customizes the configuration for network and host access. The administrator then starts the OC://WebConnect Pro emulation server and the OC://WebConnect Pro HTTP server or third-party HTTP server.

The only software on the end user desktop is the Java-enabled browser already installed for Internet or intranet access. The client software, a Java applet, is downloaded to the desktop when the end user accesses the OC://WebConnect Pro HTTP server or third-party HTTP server via a browser and starts an emulation session.

☞

Note: The client software is not installed on the desktop but is automatically downloaded from the server as needed only for the duration of the browser session.

When the OC://WebConnect Pro configuration changes or new versions become available, only the OC://WebConnect Pro server platform needs to be updated. The user desktop is automatically updated with the latest client software the next time a connection is made.

Configuration and Maintenance

OC://WebConnect Pro includes graphical interfaces for configuration and administration of server options such as port assignments, encryption choices, tracing, session status, and session kill, as well as client session configuration for host access, keyboard mapping, and color mapping. Server and client configuration and administration are provided via browser interface. An administrator can configure client sessions by either using HTML pages or dynamically downloading a Java applet.

Dynamic Interface with HTTP Servers

To dynamically provide server and session information directly from the OC://WebConnect Pro emulation server with third-party HTTP servers, a method of querying data from the server is provided. The OC://WebConnect Pro architecture uses an industry standard common gateway interface (CGI) available to most HTTP Web servers. Requests to and data from the OC://WebConnect Pro emulation server are handled by CGI processes (see connection D for **cgiinfo** in Figure 1). The CGI processes query the OC://WebConnect Pro emulation server and send configuration and server data back to the browser through the HTTP server interface (see connection C in Figure 1). The CGI process is not permanent—it lasts only long enough to get and send data for a specific request. Examples of the type of data requested are server status commands reporting on the connected sessions, list of configured and available sessions, host name and encryption option information for individual session configuration, and applet download information. The CGI interface is required only for a snapshot of the server and session status. Static HTML can be employed to download client applets.

Customization

The OC://WebConnect Pro product can be customized to incorporate OC://WebConnect Pro into an intranet or Internet Web site and provide the necessary centralized control of feature and host access. Some major areas in which OC://WebConnect Pro can be customized are HTML user interface, session level options, and emulation feature availability.

Through HTML pages, an administrator or Webmaster can control the look and feel of the initial OC://WebConnect Pro interface, the user session configurations, or the emulation features (client applets) to deliver to the end user’s desktop. The initial HTML interface and applet download can be served by either the OC://WebConnect Pro HTTP server or a third-party HTTP server.

Through customized session configuration, an administrator can create and make available a wide variety of session configurations that can vary by host, emulation configuration, level of session encryption, data stream compression, and more. These options allow the administrator to provide a product to many end-user groups, such as accounting, which might require a highly secure connection, or customers connecting via a modem, who require a quick, no-frills connection.

An administrator can provide a range of display configurations, such as keyboard mapping, color mapping, or Auto GUI interface, or can allow end users to configure their display mappings, which are stored on the user's desktop. These capabilities enable an administrator to allow more end-user control over the environment, depending on the variety and sophistication of the end users.

☞ **More Information**

For more information about OC://WebConnect Pro security, see *Chapter 15: Security Overview*.

Security

OC://WebConnect Pro provides advanced security options. Some features included are client authentication, server authentication, data encryption, and message authentication. By enabling combinations of options, varying levels of security can be established between the emulation and administration clients and OC://WebConnect Pro Server.

OC://WebConnect Pro Security Options

RC4 from RSA Data Security, Inc.

- Encrypted emulation sessions between client and server
- 40-bit encrypted key
- 128-bit encrypted key (Export restrictions apply, available in US only.)

Secure Socket Layer (SSL) from Netscape Communication

- Server authentication via X.509 certificates
- Client/server encryption algorithm negotiations
- Message authentication that protects against message tampering
- Cipher suites that provide varying levels of security

Client Token Authentication

Client authentication via a secure token-passing mechanism

☞

> **More Information**
>
> For more information about OC://WebConnect Pro security features, see *Chapter 15: Security Overview*.

Chapter 2: Starting OC://WebConnect Pro

Running the OC://WebConnect Pro Servers on UNIX

This section tells how to start and stop the OC://WebConnect Pro servers on a UNIX platform. The UNIX command-line options are also described.

Note: If OC://WebConnect Pro is not installed, refer to the *OC://WebConnect Pro Installation Guide.*

Starting the OC://WebConnect Pro Servers on UNIX

This section tells how to start and access OC://WebConnect Pro servers on a UNIX platform.

1. To start the OC://WebConnect Pro emulation server, execute **wcd** from the **wc** directory:

   ```
   ./wcd
   ```

   After the emulation server successfully starts, a series of messages are displayed showing the time the process started, the listening ports established, the server key limit, and the server process ID. Example:

   ```
   Dec 10 11:07:00 - OC://WebConnect Started    Wed Dec 10 11:07:00 1997
   Dec 10 11:07:00 - Process   27326 Started    wcd
   Dec 10 11:07:01 - Key        Session Limit:    8
   Dec 10 11:07:01 - Service    3270 Started    jcpClient
   Dec 10 11:07:01 - Service    4224 Started    apiClient
   Dec 10 11:07:01 - Process   27327 Detached   wcd
   ```

2. To start the OC://WebConnect Pro HTTP server, execute **wsd** from the **wc** directory.

   ```
   ./wsd
   ```

   After the HTTP server successfully starts, a series of messages are displayed showing the time the process started, the listening ports established, and the server process ID. Example:

   ```
   Dec 10 11:24:15 - OC://WebServer  Started    Wed Dec 10 11:24:15 1997
   Dec 10 11:24:15 - Process   29230 Started    wsd
   Dec 10 11:24:15 - Service    2011 Started    httpClient
   Dec 10 11:24:15 - Process   29231 Detached   wsd
   ```

   After the servers are active, you can access the HTTP server from a Web browser.

3. To access the *OC://WebConnect Pro* HTTP server, type the URL (Universal Resource Locator) and the port number in a Web browser.

   URL usage: **http://***hostname***:***HTTP Web server port number*

   The following example uses the default setup options:

   http://host1.oc.com:2080

   After you connect with the HTTP server through a browser, you can start emulation sessions, configure servers and sessions, and access online help.

☞

Troubleshooting

If either OC://WebConnect Pro server fails to start, use the stand-alone OC://WebConnect Pro configuration utility to reconfigure the port numbers and restart the servers. Ensure that the port assignment does not conflict with another server running on the UNIX system.

To start the OC://WebConnect Pro configuration utility from the OC://WebConnect Pro directory (default is **wc**), type the following command:

```
./configure
```

For more information about the configuration utility, see the *OC://WebConnect Pro Installation Guide* or *Chapter 5: Server Configuration and Administration*.

UNIX Command-Line Options

The command-line parameters for starting **wcd** and **wsd** are shown below:

wcd *filename* **-? -v -t** *filename* **-d** *"description"* **-l** *filename]*

wsd *filename* **-? -v -d** *"description"* **-l** *filename****]***

Note: All parameters are optional.

After OC://WebConnect Pro initializes, it detaches from the controlling terminal and returns to the command shell. The **wcd** and **wsd** commands recognize the following command-line options:

filename
: Specify the name of a file to use instead of the default server configuration file **wcd.ini**. The file must have the same format as **wcd.ini** and must be stored in the OC://WebConnect Pro directory (default directory is **wc/cfgdir/ini***)*. You could use an alternate configuration file to run a server on a different port.

-?
: Specify this option to display **wcd** and **wsd** usage information.

-d *"description"*
: Use this option to insert a textual description in the trace file, possibly to identify the trace file and the circumstances to include in the trace file. Enclose the description text in double quotes.

-l *filename*
: Use this option to redirect the OC://WebConnect Pro server's log file output to the file specified by *filename* and stored in the OC://WebConnect Pro log directory or **wc/logs** directory. By default, all log file output is sent to **stdout**. To direct output to a UNIX SYSLOG, specify **-l SYSLOG**.

-t *filename*
: **wcd** *only*. Use this option to enable the OC://WebConnect Pro daemon's trace facility. Trace information is written to the file specified by *filename*.

: You can also start a trace file remotely after the server starts through the OC://WebConnect Pro server administration panel. For more information, see *Chapter 5: Server Configuration and Administration.*

-v
: Specify this option to display OC://WebConnect Pro version information.

Stopping the OC://WebConnect Pro Servers for UNIX

To stop the OC://WebConnect Pro servers, follow these steps:

1. Determine each server's process ID. This information displays when the server starts. It also can be determined with the UNIX **ps** command:

   ```
   ps |grep wcd
   ps |grep wsd
   ```

2. Kill each server with the UNIX **kill** command:

   kill *processID*

Running the OC://WebConnect Pro Servers on Windows NT

This section tells how to start and stop the OC://WebConnect Pro servers on a Windows NT platform. Logging server activity is also described.

Note: If OC://WebConnect Pro is not installed, refer to the *OC://WebConnect Pro Installation Guide.*

Starting the OC://WebConnect Pro Servers on UNIX

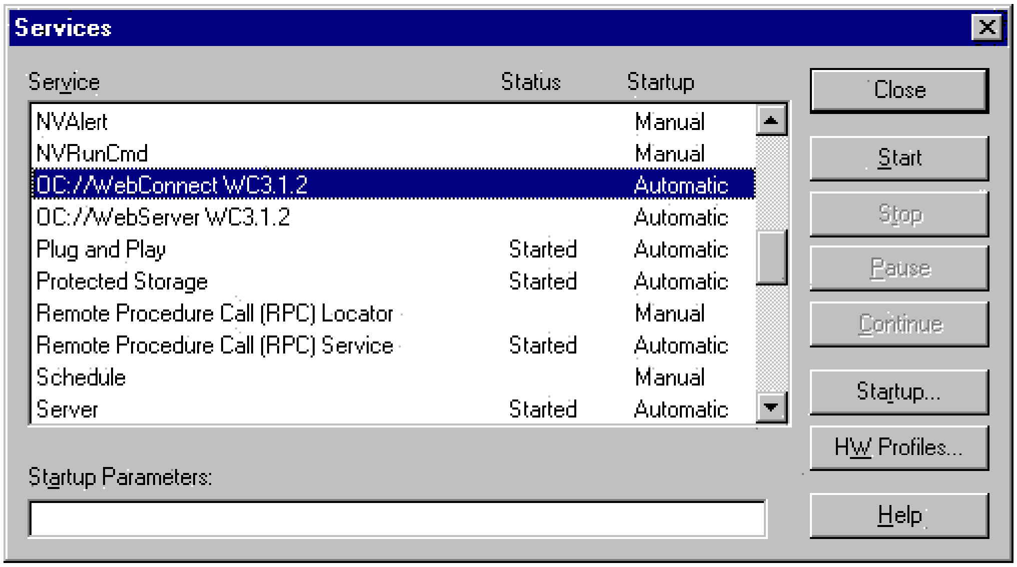
This section tells how to start and access OC://WebConnect Pro servers on a Windows NT platform.

To start the OC://WebConnect Pro servers

1. From the Windows taskbar, select **Start>Settings**>**Control Panel**.

2. Double-click **Services**.

3. To start the emulation server, select **OC://WebConnect WC*rel* #** from the list box, scrolling down if necessary, and click **Start**.



Services

Service	Status	Startup
NVAlert		Manual
NVRunCmd		Manual
OC://WebConnect WC3.1.2		Automatic
OC://WebServer WC3.1.2		Automatic
Plug and Play	Started	Automatic
Protected Storage	Started	Automatic
Remote Procedure Call (RPC) Locator		Manual
Remote Procedure Call (RPC) Service	Started	Automatic
Schedule		Manual
Server	Started	Automatic

Startup Parameters:

After the emulation server successfully starts, the Services Panel shows the OC://WebConnect Pro server status as **Started**.

4. To start the HTTP Web server, select **OC://WebServer WC*rel* #** from the list box, scrolling down if necessary, and click **Start**.

After the HTTP Web server successfully starts, the Services Panel shows the OC://WebServer status as **Started**.

5. Click the **Close** button to close the window.

To access the OC://WebConnect Pro HTTP server, type the URL (Universal Resource Locator) and the port number in a Web browser.

URL usage: **http://***hostname***:***HTTP Web server port number*

The following example uses the default setup options:

http://host1.oc.com:2080

After you connect with the HTTP server through your browser, you can start emulation sessions, configure servers and sessions, and access online help.

Troubleshooting

If either OC://WebConnect Pro service fails to start, additional error messages are logged to the Window NT Applications log.

To access the Windows NT Event Viewer:

1. Select the **Start** menu on the Windows NT taskbar.
2. Select Administrative Tools.
3. Select Event Viewer.

Use the OC://WebConnect Pro configuration utility to resolve any server configuration problems. Ensure that the port assignment does not conflict with another server running on the NT system.

To start the OC://WebConnect configuration utility:

1. Select **Start** menu on the Windows NT task bar.
2. Select **OC://WebConnect rel#.**
3. Select **OC://WebConnect Configuration Utility**.

For more information refer to the *OC://WebConnect Pro Installation Guide* or *Chapter 5 Server Configuration and Administration*.

Logging Server Activity for OC://WebConnect Pro for NT

By default, the OC://WebConnect Pro servers output only minimal messages, which are logged to the Window NT event log when services successfully start and stop. OC://WebConnect Pro can log additional server activity such as logging each session connection and disconnection, each attempt to enter the Administrative tools, and each Administrative connection. To configure this option, refer to the *OC://WebConnect Pro Installation Guide* or *Chapter 5: Server Configuration and Administration*.

To access the Windows NT Event Viewer:

1. Select the **Start** menu on the Windows NT task bar
2. Select **Administrative Tools.**
3. Select **Event Viewer**.

OC://WebConnect Pro server messages are listed in the *Applications* log.

Stopping the OC://WebConnect Pro Servers for NT

To stop the OC://WebConnect Pro servers:

1. Select **Settings** from the **Start** menu on the Windows taskbar.
2. Select **Control Panel**.
3. Select **Services**.

To stop the OC://WebConnect Pro emulation server:

1. Select **OC://WebConnect WC*rel #*** from the list box. You may have to scroll down.
2. Click the **Stop** button.

To stop the OC://WebConnect Pro HTTP Web server:

1. Select **OC://WebServer WC*rel #*** from the list box.
2. Click the **Stop** button.
3. Click the **Close** button to close the window.

Chapter 3: Navigating OC://WebConnect Pro

Overview

The OC://WebConnect Pro provides a browser-based interface made up of a series of HTML pages to launch emulation sessions, HTML pages for administration and configuration, a Java applet for configuration, and several Java applets for 3270, 5250, and VT emulation.

When a user or an administrator initially connects to the OC://WebConnect Pro HTTP server via a browser, the default **index.html** page is downloaded and displayed. The **index.html** page, or **Sessions** page, is the primary interface for end users and has links to the administration and configuration tools for an administrator. The administrative tools available from **index.html** are the HTML **Administration** and **Configuration** pages and the **GUI Configurator** Java applet. For both end user and administration, links are available for context-sensitive **Help** and an online **User’s Guide**. You can customize **index.html** as necessary.

To use OC://WebConnect Pro for starting a session, select a session configuration, set a few configuration options, and click **Start**.

To use OC://WebConnect Pro for administration and configuration, choose the **Administration** or **Configuration** buttons for HTML-based tools or the **GUI Config** button for Java-based tools. Remote administration and configuration tools require an administrator password.

The **Help** provides context-sensitive HTML help pages.

The **User’s Guide** button provides HTML documentation for both the administrator and end user.

General HTML Page Layout

Each OC://WebConnect Pro HTML page has at least three frames or sections:

- On the top is the header section, which shows the OC://WebConnect Pro version accessed and the name of the HTML page displayed, for example, **Sessions**, **3270 Configuration**.
- On the left are navigation buttons, which are links to access other OC://WebConnect Pro HTML pages or Java applets. These navigation buttons differ for each HTML page. For example, the **Sessions** page includes links for **Administration**, **Configuration**, and **GUI Config** (configuration), as well as context-sensitive help and the online User's Guide. A configuration page includes links to save or cancel the configuration changes and links to other more specific configuration pages.
- The main section to the middle and right is the selection and input section, where choices and input fields are displayed for the end user or administrator to select options and enter information. Buttons are included for functions like **Edit**, **Copy**, and **Delete**.

Sessions Page

The OC://WebConnect Pro default page has three sections:

- On the top is the header section, which shows the version of OC://WebConnect Pro accessed and the name of the HTML page displayed, **Start Sessions**.
- On the left are navigation buttons to access other OC://WebConnect Pro HTML pages for **Administration**, **Configuration**, and **GUI Config** (configuration), as well as context-sensitive help, the online **User's Guide**, and a screen **Refresh** button.
- To the middle and right is the section used to select and start sessions.

Header Section

The header section displays the OC://WebConnect Pro logo, version number, and **Start Sessions** to identify the HTML page.

Navigation Buttons

Administration	Perform HTML administrative functions such as viewing server settings or server status, deleting emulation sessions; or starting, stopping, or viewing traces.
Configuration	Create, modify, or delete sessions and session features with HTML configuration. Server ports can also be reconfigured via this button.
GUI Config	Create, modify, or delete sessions and session features and server ports using the graphical GUI Configurator.
Help	Access context-sensitive help.
User's Guide	Access online user guide.
Refresh	Refresh the list of session configurations.

Session Select and Start Section

This section of the **Sessions** page includes a list of available session configurations, a choice of applet types, a choice to enable SSL security, and a choice of print methods for print screen or 3287 printing.

The **Sessions** list shows sessions available to start, including the default sessions originally configured during installation (default 3270, 5250, VT, and 3287) and any additional sessions created by the administrator. See *Chapter 4: Starting an Emulation Session* for more details.

The applet type list box shows available applet types:

- **Ultra Lite** enables all functions available in OC://WebConnect Pro version 2.6. This applet works with any browser that supports Sun’s JDK 1.0 and above.

  Note: SSL is not supported for this setting.

- **Enhanced** contains the features available in OC://WebConnect Pro version 3.1, including print, copy, paste, and hot spots. A browser that supports Sun’s JDK 1.1 is required.

- **Power User** contains the features available in OC://WebConnect Pro version 3.1, as well as IND$FILE transfer and Auto GUI features. A browser that supports Sun’s JDK 1.1 is required.

The SSL list box gives the end user the option to start a session using SSL authentication and encryption. The OC://WebConnect Pro emulation server can be configured to require the session to use SSL.

- **SSL Disabled**

- **SSL Enabled**

The Print method list box allows the end user to use the default print method specified in the session configuration or to override the session configuration.

- **Default Print** uses the print option defined in the session (**.ses**) file used for the session.
- **OC://WebPrint** uses the OC://WebPrint solution for print screen function. OC://WebPrint must be installed on the browser platform to use this feature. This is supported on JDK 1.0 and greater browsers.
- **JavaScript** is a print screen option embedded in some browsers. This option is supported in some JDK 1.0 and greater browsers.
- **JDK 1.1** print screen method is embedded in JDK 1.1**-**based browsers only.
- **Disabled** turns off the screen print capability.

Starting an Emulation Session

When starting a session, the user has four items to select before clicking the **Start** button.

1. Highlight the session to start.
2. Choose an applet type: **Ultra Lite, Enhanced,** or **Power User**.
3. Choose whether to use **SSL Enabled** or **SSL Disabled** (Secure Socket Layer). The default is **SSL Disabled**. See *Chapter 13: Security Features* for more details.
4. Choose a printing option.
5. Click **Start** to download the emulation applet and start an emulation session.

☞

More Information

A customized session screen (HTML page) can be created listing only the sessions available to users in your organization. See *Chapter 12: Customization of OC://WebConnect Pro* for more details.

Administration Pages

The **Administration** button is used for performing a variety of OC://WebConnect Pro HTML administration tasks.

Enter the appropriate password in the **Administrator Password** field and click **OK**. The default password is **OCS** (uppercase).

Note: Because this password is documented, it is recommended that the administrator password be changed from the default.

When the correct administrator password is entered, the main **Administration** HTML page is displayed.

Navigation Buttons

Server...	View the server status and shut down and restart the OC://WebConnect Pro server.
Sessions...	View client session status and kill individual sessions.
Tracing...	Start, stop, view, download. and delete traces.
Help	Access context-sensitive help.
User's Guide	Access the online user guide.
Done	Exit session configuration.

☞

More Information

For more information on the OC://WebConnect Pro status pages, restarting the server, killing sessions, and tracing, see *Chapter 5 Server Configuration and Administration*.

Configuration Pages

The **Configuration** button is used to configure sessions and the OC://WebServer.

Enter the appropriate password in the Administrator Password field and click **OK**. The default password is **OCS** (uppercase).

Note: Because this password is documented, it is recommended that the administrator password be changed from the default.

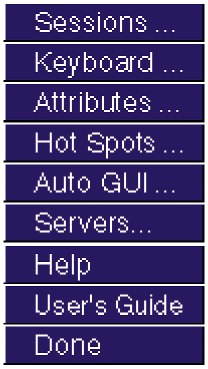
When the correct administrator password is entered, the main **Configuration** HTML page is displayed.

More Information

For more information about emulation features and creating, configuring, editing, or deleting session, refer to one of the following :

- *Chapter 6: Configuring 3270 Emulation Sessions*
- *Chapter 7: Configuring 5250 Emulation Sessions*
- *Chapter 8: Configuring 3287 Print Sessions*
- *Chapter 9: Configuring VT Emulation Sessions*

Navigation Buttons



Sessions ...	Configure an individual session.
Keyboard ...	Create, modify, or delete a keyboard map.
Attributes ...	Create, modify, or delete an attribute and color map.
Hot Spots ...	Create, modify, or delete a Hot Spot map.
Auto GUI ...	Create, modify, or delete a Auto GUI map.
Servers...	Modify server settings.
Help	Access context-sensitive help.
User's Guide	Access the online user’s guide.
Done	Exit session configuration.

Sessions, Keyboard, Attributes, Hot Spots, and Auto GUI

A list of existing session configurations is displayed. To edit, copy, or delete an existing session, select a session and click a button. A group of radio buttons shows supported emulation types. To create a new session, choose an emulation type and click **New**.

Servers

Click **Server** to edit the OC://WebConnect Pro port configuration.

GUI Configurator Applet

After the OC://WebConnect Pro server starts, the GUI Configuration applet can be accessed through the **GUI Config** button on any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser. See *Chapter 2: Starting OC://WebConnect Pro.*

Administrator Mode Versus User Mode

The GUI Configuration applet can be started in either user mode or administrator mode. This is determined by the **Allow User Configuration** option explained below.

- When **Allow User Configuration** is not enabled, the GUI Configuration applet starts in administrator mode and is password protected. When the correct password is entered, the full GUI Configuration utility starts.
- When **Allow User Configuration** is enabled, the GUI Configuration applet starts in user mode, and the user is not prompted for a password. The GUI Configuration for end user is displayed, and all changes are written to the browser platform, not the server.

The administrator mode, protected by password, is accessible through the user mode.

Using the GUI Configurator in Administrator Mode

After the GUI Configuration applet is downloaded to the browser, the **Configuration Permissions Dialog** window displays asking for the administrator password.

1. Enter the appropriate password in the **Administrator Password** field.
2. Click **OK**. The OC://WebConnect Pro **GUI Configurator** window displays in Administrative mode.

   -or-

   Click **Cancel** to return to the main OC://WebConnect Pro HTML page.

When the correct administrator password is entered, the GUI Configuration applet appears with the current configuration information including four tabs. The tabs and their functions are shown below:

OC://WebConnect Pro Server
Modify IP addresses.
Modify port numbers.
Set GUI Configurator Cipher Suite.
Allow User Configuration.
Conceal Host Connection Information.
Enable Client Token Authentication and Timeout.
Set Client Are You There Timeout.
Submit changes to save modifications.

Password
Set New Administrator Password.

License Key
Enter new software authorization key.

Sessions
Create Sessions.
Delete Sessions.
Edit existing session configuration properties.

☞

More Information

For more information on the OC://WebConnect Pro Server, Password, and License Key tabs see *Chapter 5 Server Configuration and Administration*.

Help

Help displays the OC://WebConnect Pro context-sensitive help for the current page. A separate HTML page opens with information related to the current OC://WebConnect Pro page.

User’s Guide

The **User’s Guide** provides access to the OC://WebConnect Pro online documentation. A separate browser instance opens containing an outline with links to the various areas of the documentation.

Chapter 4: Starting an Emulation Session

Overview

OC://WebConnect Pro provides a default HTML interface, accessed via a browser, to start an emulation session. This interface allows emulation client users to select an emulation session configuration and then automatically downloads the emulation software, starts a client session, and connects to a S/390, AS/400, or UNIX host.

Like most Web-based products, the initial interface to the product is an **index.html** page. By specifying the OC://WebConnect Pro URL (host name and port) in the browser, you can contact the HTTP server and, by default, download an HTML page named **index.html**.

For the OC://WebConnect Pro product, the default **index.html** page is the **Start Sessions** page. The **Start Sessions** page displays the available emulation client session configuration, a list of emulation client applet packages, a choice of print methods, an option to enable or disable SSL security, and a **Start** button to start a session.

The emulation client end user can select a session and click Start. A Java applet is downloaded to the browser platform, the applet is started by the browser, and a connection is made to the host configured for that session.

Buttons to access context-sensitive **Help**, an online User's Guide and administrative and configuration tools are also available on the **Start Sessions** HTML page.

The OC://WebConnect Pro **index.html** page can be replaced with a customized **index.html** page. The default **index.html** page is available as an example and as a tool for demonstrating and evaluating OC://WebConnect Pro. It can also be used in a production environment. Some administrators customize **index.html** to limit end users access to administration and configuration tools, restrict the ability of an end user to select session configurations, or just change the look and feel of the page to blend with the corporate Web site. In addition to customizing the **index.html** page, a third-party HTTP server can be used rather than the OC://WebConnect Pro server.

☞

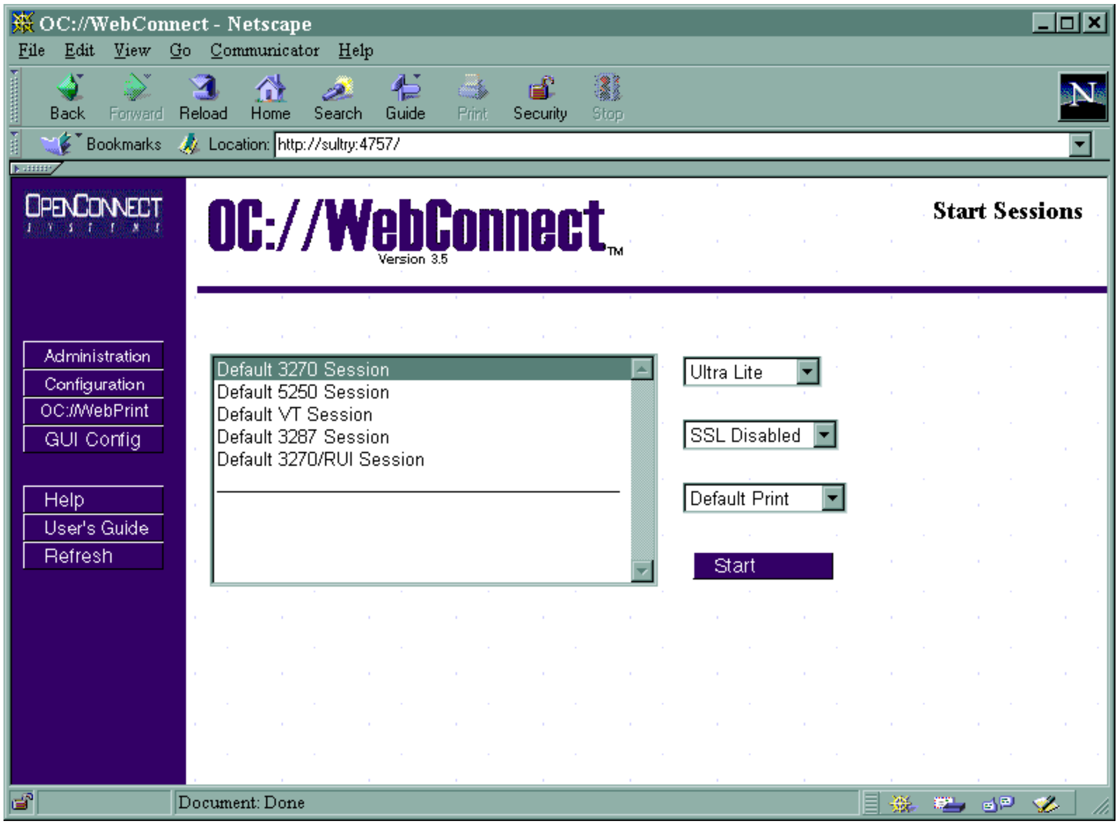
More Information

For more information about Customization of OC://WebConnect Pro, see *Chapter 12: Customizing OC://WebConnect Pro*.

Sessions Page Layout

The **Sessions** page has three sections, the header section, navigation section, and the session select and start section:

- The header section at the top shows version information and identifies the HTML page as the **Start Sessions** page.
- The navigation section, to the left, provides links to OC://*WebConnect Pro* administration and configuration tools, context-sensitive help, an online User's Guide. A window **Refresh** button is also provided.
- The session select and start section is the main section at the right of the navigation section. A list box shows emulation session configurations. When OC://*WebConnect Pro* is first installed, only the default session configurations are listed. As the administrator adds, modifies, and deletes session configurations, this list automatically changes. Another list shows the OC://*WebConnect Pro* applet types: **Ultra Lite**, **Enhanced**, and **Power User**. A third list box allows enabling or disabling **SSL** security. The last list box shows available print solutions. An end user can override the session configuration by choosing **OC://WebPrint**, **JavaScript**, **JDK 1.1**, or **Disabled**. The **Start** button downloads and starts a OC://*WebConnect Pro* Java emulation client based on the choices made.


OC://WebConnect - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://sultry:4757/
OPENCONNECT SYSTEMS
OC://WebConnect™ Version 3.5
Start Sessions
Administration
Configuration
OC://WebPrint
GUI Config
Help
User's Guide
Refresh
Start
Document: Done

Default 3270 Session
Default 5250 Session
Default VT Session
Default 3287 Session
Default 3270/RUI Session

Ultra Lite

SSL Disabled

Default Print

Starting an Emulation Session

The steps below describe how to start an emulation session using the **Start Sessions** page provided with OC://*WebConnect Pro* in the form of the **index.html** file. If the **index.html** file has been customized, the steps described might not work.

1. Access the **Select Sessions** window by entering the URL of the OC://*WebConnect Pro* HTTP server into a browser and hit return. Example:

   http://host1.oc.com:2080

2. The default **Sessions** page is displayed. A list of available session configurations is displayed.

   The list of available session configurations is the responsibility of the OC://*WebConnect Pro* administrator. The administrator should create, modify, or delete sessions as necessary to meet the end user needs. The description of each session configuration is entered by the administrator and should be a description meaningful to end users.

3. Select a session configuration. A list of OC://*WebConnect Pro* applet packages is displayed.

4. Choose an emulation client applet package. The **Ultra Lite**, **Enhanced**, and **Power User** emulation applet packages are available to meet different user environments and needs.

   - **Ultra Lite** enables all functions available in OC://*WebConnect Pro* version 2.6. This applet works with any browser that supports Sun's JDK 1.0 and above.

   - **Note:** SSL is not supported for this setting.

   - **Enhanced** contains the features available in OC://*WebConnect Pro* version 3.1, including print, copy, paste, and hot spots. A browser that supports Sun's JDK 1.1 is required.

   - **Power User** contains the features available in OC://*WebConnect Pro* version 3.1, as well as IND$FILE transfer and Auto GUI features. A browser that supports Sun's JDK 1.1 is required.

5. Choose whether to enable SSL authentication and encryption for this session connection. This choice is a security versus time consideration. For more information about SSL, see *Chapter 15 Security Overview*.

6. The print method list box shows available print solutions for screen print or 3287 print.

   - **Default Print** uses the print option defined in the session (**.ses**) file being used for the session.

   - **OC://WebPrint** uses the OC://WebPrint solution for print screen functionality. OC://WebPrint must be installed on the browser platform to use this feature. This is supported on JDK 1.0 and greater browsers.

   - **JavaScript** is a print screen option embedded in some browsers. This option is supported in some JDK 1.0 and greater browsers.

   - **JDK 1.1** print screen method is embedded in JDK 1.1-based browsers only.

   - **Disabled** turns off the screen print capability for this session.

7. Click the **Start** button. The following sequence of events occurs:

   a. A Java emulation applet is downloaded into the memory of the browser platform the first time the applet package is chosen during the browser session. Additional applet starts do not require another download.

   b. While the applet downloads, the browser displays information about the files being downloaded in a status line usually at the bottom of the browser window.

   c. When the applet download completes, the browser starts the applet and the applet window is displayed.

   d. Once the applet starts, the emulation client automatically makes a connection with the OC://WebConnect Pro emulation server.

e. If RSA encryption has been chosen, encryption keys are generated and exchanged. All data between the emulation client applet and the OC://WebConnect Pro emulation server is encrypted.

f. The OC://WebConnect Pro emulation server connects to the S/390, AS/400, or UNIX host specified in the session configuration.

g. Emulation data begins to flow, and the host data is displayed in the emulation client applet window.

☞

More Information

For more information about emulation client features and how to choose the appropriate emulation client type, see Chapter 11 Emulation Client Interface and Features.

Chapter 5: Server Configuration and Administration

Overview

OC://WebConnect Pro provides three methods for configuring and administering OC://WebConnect Pro servers and sessions:

- The OC://WebConnect Pro configuration utility is a limited, stand-alone UNIX or NT script. It is used prior to starting the OC://WebConnect Pro servers to configure server ports and IP addresses, minimum default session settings, server language, sensitive security settings, and default HTML files. The OC://WebConnect Pro configuration utility does not require a browser.

- The HTML administration and configuration is a remote method of configuration that uses the running OC://WebConnect Pro server via a browser. HTML pages and a common gateway interface (CGI) are used to configure and administer OC://WebConnect Pro servers and sessions. HTML administration and configuration does not require a Java-enabled browser.

- The graphical **GUI Configurator** is a Java applet. The **GUI Configurator** is also a remote method that involves the download and execution of a Java applet via a enabled JDK 1.1 Java-enabled browser.

The HTML administration and configuration utility and the GUI Configurator both provide full-featured configuration. The two methods are provided for the differing needs and preferences of OC://WebConnect Pro users.

OC://WebConnect Pro Configuration Utility

The OC://WebConnect Pro configuration utility is a stand-alone UNIX script or NT program used to configure the OC://WebConnect Pro servers and default sessions prior to starting the OC://WebConnect Pro servers. The configuration utility must be executed from the platform on which OC://WebConnect Pro is installed.

The following items can be configured using the configuration utility:

- OC://WebConnect Pro emulation server ports.
- OC://WebConnect Pro HTTP or HTTPS server port or both.
- Host names and ports for the default 3270, 5250, 3287, and VT session configurations.
- Server license key.
- Server or administration language (English, German, French, or Castilian Spanish).
- Secure Socket Layer (SSL) key pair, SSL password, and enabling/disabling SSL.

  Note: Key generation is provided only via the configuration utility.
- HTML used to access, configure, and administer the OC://WebConnect Pro servers and to download emulation sessions.

For security reasons, the OC://WebConnect Pro configuration utility is not provided through a browser connection.

Using the Configuration Utility for UNIX

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

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

   ./configure

The following menu is displayed:

```
1)    Configure 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 WebServer Ports
9)    Configure WebConnect SSL
0)    Exit
```

2. Select the number of each configuration option, as needed. The configuration items are discussed below. When configuration of all options is complete, the OC://WebConnect Pro HTML files are automatically updated. This is relevant for anyone using the OC://WebConnect Pro-provided HTML files either directly or as a model for customization. All files in the OC://WebConnect Pro **html** directory are scanned for host name, port parameters, and server language, and 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 Pro via a browser, start an emulation session, or retrieve server status information.

   Note: If you press the **Return** key each time the main menu is displayed, the configuration automatically steps through each menu item.

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

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

Using the Configuration Utility for Windows NT

To configure OC://WebConnect Pro using the OC://WebConnect Pro configuration utility:

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

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

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

4. Select the number of each configuration option, as needed. The configuration items are discussed below. Current configuration information is displayed.

5. Press **Return** to accept the current information or change the information as needed.

   When configuration of all options is complete, the OC://WebConnect Pro HTML files are automatically updated. This is relevant for anyone using the OC://WebConnect Pro-provided HTML files either directly or as a model for customization. All files in the OC://WebConnect Pro

html directory are scanned for host name, port parameters, and server language, and 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 Pro via a browser, start an emulation session, or retrieve server status information.

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

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

OC://WebConnect Pro Configuration Options

1) Configure WebConnect Ports

Each OC://WebConnect Pro 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 Pro servers to respond to requests from all installed network interfaces. Specify another IP address to limit OC://WebConnect Pro to one network interface.

OC://WebConnect Pro emulation server can use up to three ports during operation. The default port setting can be used, or the port can be changed to a number greater than 0 and less than 65,535. Root privileges are required to use a port number less than 1024. A port number of 0 disables a port.

The default settings are described in the following table.

Port Number	Service	Description
3270	Java Server	Listening port for non-SSL Java emulation clients. *Required*.
3443	Secure Java Server	Listening port for SSL Java emulation and administration clients. *Optional* if not using SSL.
4270	Java Administration	Listening port for CGIbin interface to obtain configuration parameters for launching applets and for retrieving server status information. *Optional* if using static HTML and not reporting server status information.

For more information about ports, see “Server Ports.”

2) Configure Default 3270 Session

This selection configures the domain name server (DNS) host name or IP address and TCP port address of a TN3270 server, TN3270E server, or gateway for mainframe emulation 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 Pro HTML configuration or OC://WebConnect Pro GUI Configurator.

3) Configure Default 5250 Session

This selection configures the 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 5250 sessions can be configured later using the OC://WebConnect Pro HTML configuration or OC://WebConnect Pro GUI Configurator.

4) Configure Default VT Session

This selection configures 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 VT session configuration. Other default session settings and additional VT sessions can be configured later using the OC://WebConnect Pro HTML configuration or OC://WebConnect Pro GUI Configurator.

5) Configure Default 3287 Session

This selection configures the DNS host name or IP address and TCP port address of a TN3270 server, TN3270E server, or gateway for mainframe print emulation access. This information is used to create the default 3287 Print session configuration. Other default session settings and additional 3287 sessions can be configured later using the OC://WebConnect Pro HTML configuration or OC://WebConnect Pro GUI Configurator.

6) Configure License Key Information

OC://WebConnect Pro comes prepackaged with a license key to enable the server for a specific number of concurrent sessions and key expiration. Press **Return** to accept the default key. If a special or replacement key has been provided, enter the key at this time. The number of concurrent sessions and expiration date for the key configured can be seen when the OC://WebConnect Pro servers are started, on the OC://WebConnect Pro Status page, log file, or trace file.

7) Configure Default Administration Language

OC://WebConnect Pro can be configured to one of four possible server languages. The OC://WebConnect Pro server language is used for the HTML configuration pages, the GUI Configurator client, the OC://WebConnect Pro HTML session selection pages, and online user’s guide. When the server language is changed, the HTML files provided with OC://WebConnect Pro are automatically updated and include any previously configured server host names or ports.

For more information about ports, see “Server Ports.”

8) Configure WebServer Ports

The OC://WebConnect Pro HTTP Web server can listen to incoming requests on one or all network interfaces installed on a UNIX platform. The configuration utility lists all IP addresses for the network interfaces detected and defaults to 0.0.0.0, which causes OC://WebConnect Pro servers to respond to requests from all installed network interfaces. Specify another IP address to limit OC://WebConnect Pro to one network interface.

To use the OC://WebConnect Pro Web servers, type a TCP port number for the HTTP or HTTPS server or both. One of these port numbers is used when accessing OC://WebConnect Pro via a browser. Examples:

```
http://host1.oc.com:2080
https://SSL-host1.oc.com:2443
```

The default OC://WebConnect Pro HTTP Web server port is 2080 for the HTTP server and 2443 for the HTTPS server. Many HTTP Web servers use ports 80 and 443 for HTTP and HTTPS, respectively. Because most browsers default to ports 80 and 443, the browser user only enters the Web server host name and not a port. Examples:

```
http://host1.oc.com
https://SSL-host1.oc.com
```

A port number of 0 for either server disables the respective service.

For more information about ports, see “Server Ports.”

9) Configure WebConnect SSL

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

Note: The OC://WebConnect Pro server and HTTP Web server use the same key pair and certificate.

If a key pair and certificate is generated, answer YES to enable SSL and make it fully operational when the OC:/WebConnect Pro 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 from the CA, manually installed in the OC://WebConnect Pro security directory, and the configuration utility is rerun to enable SSL.

When executing the configuration utility after installing the certificate, answer NO when asked to generate a new key pair; then answer YES when asked to enable SSL.

SSL Key Pair and Certificate Generation

OC://WebConnect Pro 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 Pro server. Each panel presents detailed information concerning a particular question, followed by the actual question.

For optimal performance and 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 step 2 and proceed to directly step to 3.

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

This question is only relevant if exportable(40-bit) ciphers will be used with this installation. If "yes" is chosen, a 512-bit key will be used for these ciphers, rather than waiting until session startup. This will improve session connect times and help 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 will need to type in this password each time OC://WebConnect Pro is started, making unattended restarts impossible, unless the password is stored on the server system. 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 Pro 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 the password is entered, the RSA key pair is generated. This can take anywhere from a couple of 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 a server-wide key exchange key pair was selected.

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: [host name]
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 will 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 will be 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 are accurate. Spell out the **State**.

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 Pro 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 Pro server certificate. The setup for server authentication will be handled automatically if the default method is chosen and the OC://WebConnect Pro provided CGIbin for applet startup is used.

Alternatively, if No is chosen only a certificate request is generated. The request will have to submitted to a CA and manually install the certificate into the security directory and rerun configure. With a CA-generated certificate, it may be desirable for the 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 determines the expiration date of the certificate.

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

8. *More information is needed 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** subdirectory of the OC://WebConnect Pro home directory. After the certificate is installed, rerun the configuration utility to enable SSL.

To make OC://WebConnect Pro clients validate to the CA rather than the server certificate, recreate the HTML 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.

Client Authentication

Client authentication using SSL/X.509 certificates is one of the most secure mechanisms available to guarantee that only valid users can access a given server. For the highest possible security with OC://WebConnect Pro, activate SSL in both servers and use client authentication accompanied by the token authentication feature.

In OC://WebConnect Pro, client authentication is activated by setting the **Require HTTPS client authentication** option in the security section of server configuration. This causes the OC://WebConnect Pro HTTPS server to request a certificate from the connecting browser as part of the SSL protocol. If the browser cannot produce a valid certificate signed by a Certification Authority (CA) known by the server, then the server denies access to the user by disconnecting the browser.

To take advantage of the client authentication feature, you need to have a CA issue certificates for each user and browser. The CA can be created and operated by your organization using a third-party CA product such as XCert Sentry CA, Netscape Certificate Server or Entrust Web CA, or you can use the services of a trusted third-party CA such as Verisign.

OC://WebConnect Pro supports X.509 V3 certificates using the RSA signing algorithm with MD5 or SHA-1. In general, certificate extensions are not supported.

To configure OC://WebConnect Pro to accept the browser certificates, install the CA certificates or the individual client certificates in the server's client database. In OC://WebConnect Pro, this is a flat file named **certsacc.txt** installed in the **security** subdirectory of the OC://WebConnect Pro installation. The certificates must be DER-formatted, base 64-encoded, and delimited by the following lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

If you install the certificate of the issuing CA, then any browser with a certificate issued by this CA will be allowed to connect. For this reason, an internal CA typically gives you more control of your security.

If you need the server to reject specific certificates issued by a configured CA, you can do this, too. Create a file containing these certificates named **certsrej.txt** and install it in the **security** subdirectory of the OC://WebConnect Pro installation. The format of this file is identical to the **certsacc.txt** file.

Note: A browser must support client authentication via X.509 certificates to utilize this feature. Consult the documentation of the browser or CA for instructions on how this is done for a particular browser. You can also reference the following links for information concerning Netscape and Microsoft products:

http://home.netscape.com/client.html
http://home.netscape.com/eng/security/downloadcert.html
http://www.microsoft.com/security/ca/howto.htm

OC://WebConnect Pro HTML Administration

The OC://WebConnect Pro HTML administration and configuration HTML pages provide the ability to administer and configure the OC://WebConnect Pro emulation server and emulation sessions. The OC://WebConnect Pro emulation server must be running to use these tools. Using the HTML administration pages, you can remotely administer the following options:

- Restart the OC://WebConnect Pro emulation server.
- Enable or disable OC://WebConnect Pro tracing or view traces.
- Shut down OC://WebConnect Pro emulation server.
- Display the status of all current sessions.
- Kill individual emulation sessions.

More Information

The **Administration** button can be removed from any OC://WebConnect Pro HTML page, or custom HTML can be written to access the GUI configuration applet. See *Chapter 12: Customizing OC://WebConnect* for more information.

Using the HTML Administration HTML Pages

After the OC://WebConnect Pro server starts *(s*ee *Chapter 2: Starting OC://WebConnect Pro)*, you can access the HTML administration pages via a browser by selecting the **Administration** link on the main *OC*://WebConnect Pro HTML pages.

1. Connect to the OC://WebConnect Pro HTTP Web server by typing the host name and TCP port number in the URL of a browser. Example:

   http://host1.oc.com:2080

2. Click **Administration** on the left side of the **Start Sessions** page. A prompt appears to **Enter Administrator Password**.

3. Enter the appropriate password and click **OK**. The default password is **OCS**. Because this password is documented, it is recommended that it be changed as soon as possible.

   The HTML **Administration** page, showing the **Server Status**, is displayed.

HTML Administration Page Layout

The HTML **Adminstration** page has three frames or sections, the header, navigation buttons, and administration sections.

At the top is the header section, which shows the OC://WebConnect Pro version accessed and the name of the HTML page displayed, **Administration Server Status** in this case, in the upper right corner.

On the left are navigation buttons (**Server**, **Sessions**, **Tracing**, and, optionally, **Access Control**) to access other OC://WebConnect Pro HTML pages. The **Access Control** option appears if **Access Control** is selected when configuring the server. See “Setting Server Security Options” in this chapter.

To the middle and right is the administration section, which displays information about the current server status and current users. Buttons are provided to restart the server, shut down the server, kill current sessions, and enable, disable, or view tracing.

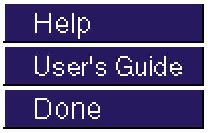
Navigation Buttons

Server – Display the OC://WebConnect Pro emulation server status, restart the server, or shut down the server.

Sessions – Display the sessions currently connected to the OC://WebConnect Pro server or kill individual sessions.

Tracing – Enable, disable, or view tracing.

Access Control – Override default session parameters by user ID.



Access context-sensitive help.

Access the online user guide.

Exit administration pages.

Server Status

The **Server Status** page includes information about the OC://WebConnect Pro emulation server and the ability to restart or shut down the OC://WebConnect Pro emulation server. The following table describes the information on this panel.

Field	Description
Host	The DNS host name or IP address where the OC://WebConnect Pro emulation server is running.
Server Version	The version of the OC://WebConnect Pro emulation server.
Started	The time the current instance of the OC://WebConnect Pro emulation server was started.
UpTime	The elapsed time between the current time and the time the OC://WebConnect Pro emulation server started.
Key Expiration	The date on which the user license for OC://WebConnect Pro expires.
Process ID	The UNIX process ID for the OC://WebConnect Pro emulation server.
Session Limit	The maximum number of concurrent emulation sessions.
Active Sessions	The number of sessions currently connected to the OC://WebConnect Pro emulation server, including emulation and configuration sessions.

Session Status

The **Session Status** page includes information about all sessions currently connected to the OC://WebConnect Pro emulation server and the ability to kill one or more session connections. The following table describes the information on this panel.

Field	Description
Kill	This box marks a session to be killed. Use the kill session button to kill all the marked sessions.
ID	The OC://WebConnect Pro ID for this session. This ID corresponds to the ID in trace files.
Type	The type of session connection. Example: CGI-BIN, 3270, 5250.
IP Address	The IP address of the workstation on which the emulation or configuration session is running.
Connect Time	The date and time the session connection was made.
Last Response	The last time a response from the session was received by the server.
Bytes Sent	The number of bytes sent from the session to the OC://WebConnect Pro server.
Bytes Received	The number of bytes received by the session from the OC://WebConnect Pro server.

Tracing

The **Tracing** page provides a facility for starting and stopping an OC://WebConnect Pro trace while the server is running. On this HTML page, trace files can also be viewed and deleted.

Controlling Session Access

The **Access Control** page is available if **Access Control** is enabled when configuring the server. Access control allows you to override default session parameters for specific user IDs. See “Setting Server Security Options” in this chapter. The **Access Control** page lists user IDs currently under access control and provides buttons to add a user ID to access control, edit a user ID, or delete a user ID. When you select **Edit** or **New**, you can change or add information to the fields described below.

Field	Description
User ID	The user ID for this instance of access control.
Password	*Optional*. The password for the user ID.
Prompt user for new password	*Optional*. If checked, user is asked to change the password at the next logon.
Session	The session type to override. Select None or a specific session type.
Host	*Optional*. Host to connect to for this session.
Port	*Optional*. Port the host is listening on.
LU Name	*Optional*. Specific LU to connect to.

Displaying Server Status

To display the OC://WebConnect Pro emulation server status:

1. Select the **Administration** button from the **Start Sessions** HTML page.
2. Enter the administrator password. The **Server Status** page displays.

Restarting the Server

To restart the OC://WebConnect Pro emulation server:

1. Select the **Administration** button from the **Start Sessions** HTML page.
2. Enter the administrator password. The **Server Status** displays.
3. Select the **Restart Server** button.

   Note: All sessions connected to the OC://WebConnect Pro server are disconnected when the server is restarted, including the administration session.

Shutting Down the Server

To shut down the OC://WebConnect Pro emulation server:

1. Select the **Administration** button from the **Start Sessions** HTML page.
2. Enter the administrator’s password.
3. The Server status should display
4. Select the **Shutdown Server** button. All sessions connected to the OC://WebConnect Pro server are disconnected when the server is shut down, including the administration session. The server will have to be restarted from the UNIX command line or the NT Services panel.

Displaying Current Session Status

To display the status of the sessions currently connected to the OC://WebConnect Pro server :

1. Select the **Administration** button from the **Start Sessions** HTML page.
2. Enter the administrator’s password.
3. Choose the **Sessions** button. The **Session Status** page displays.

Killing a Current Session

To kill a session currently connected to the OC://WebConnect Pro server:

1. Select the **Administration** button from the **Sessions** HTML page.
2. Enter the administrator’s password.
3. Choose the **Sessions** button. The Session status page displays.
4. In the **Kill** column next to each session, mark the sessions to be killed.
5. Choose the **Kill Session** button.

Starting an OC://WebConnect Pro Trace

1. Select the **Administration** button from the **Sessions** HTML page.
2. Enter the administrator password.
3. Choose the **Tracing** button. The Tracing page displays.
4. Enter a filename for the new trace file.
5. Choose the **Start Tracing** button.

Viewing an OC://WebConnect Pro Trace

1. Select the **Administration** button from the **Start Sessions** HTML page.
2. Enter the administrator password.
3. Choose the **Tracing** button. The Tracing page displays.
4. Choose a trace file from the list of trace files.
5. Choose the data to view: JCP, Telnet/RUI, HTTP, or Session ID.
6. Choose the **View Trace** button.

Adding User Access Control

Note: This feature is available only if access control was selected during server configuration. See "Setting Server Security Options" in this chapter.

1. From the **Start Sessions** HTML page, click **Administration** on the left side of the page. The **Enter Administrator Password** window displays.

2. Type the correct administrator password and click **OK**. The **Administration Server Status** window displays.

3. Click **Access Control** on the left side of the page. The list of users currently under access control displays.

4. Click **New**. A window with blank fields appears.

5. In the **User ID** field, type the ID of the user to add.

6. Type the information, as needed, in the other fields to override default session parameters.

7. Click **Save** to add the user access control. The override information for the user ID is saved and appears in the list of users under access control.

   -or-

   Click **Cancel** to return to the previous window without saving the information.

Changing User Access Control

Note: This feature is available only if access control was selected during server configuration. See "Setting Server Security Options" in this chapter.

1. From the **Start Sessions** HTML page, click **Administration** on the left side of the page. The **Enter Administrator Password** window displays.

2. Type the correct administrator password and click **OK**. The **Administration Server Status** window displays.

3. Click **Access Control** on the left side of the page. The list of users currently under access control displays.

4. Select the user ID to change and click **Edit**. The current information for the user ID displays.

5. Change or add information, as needed, to override default session parameters.

6. Click **Save** to save the changes. The override information for the user ID is saved.

   -or-

   Click **Cancel** to return to the previous window without saving the information.

Deleting User Access Control

Note: This feature is available only if access control was selected during server configuration. See "Setting Server Security Options" in this chapter.

1. From the **Start Sessions** HTML page, click **Administration** on the left side of the page. The **Enter Administrator Password** window displays.
2. Type the correct administrator password and click **OK**. The **Administration Server Status** window displays.
3. Click **Access Control** on the left side of the page. The list of users currently under access control displays.
4. Select the user ID to delete.

   Click **Delete** to delete the user ID. The override information for the user ID is deleted from the list.

OC://WebConnect Pro HTML Configuration

The OC://WebConnect Pro HTML configuration HTML pages provide the ability to configure the OC://WebConnect Pro emulation server and emulation sessions. The OC://WebConnect Pro emulation server must be running to use these tools. Using the HTML configuration pages, you can remotely configure the following options:

- Modify the OC://WebConnect Pro emulation server ports.
- Modify OC://WebConnect Pro administration ports.
- Select Cipher suites.
- Configure to conceal host connection information from client emulation users.
- Enable and configure Client Token authentication.
- Modify the administration password.
- Modify the server license key.

☞

More Information

The **Configuration** button can be removed from any OC://WebConnect Pro HTML pages, or custom HTML can be written to access the GUI Configurator applet. See *Chapter 12: Customizing OC://WebConnect Pro* for more information.

HTML Configuration Page Layout

After the OC://WebConnect Pro server starts *(*See *Chapter 2: Starting OC://WebConnect Pro)*, the HTML configuration pages can be accessed via a browser by selecting **Configuration** on the main OC://WebConnect Pro HTML pages.

The HTML server configuration page has three frames or sections: the header, navigation buttons, and configuration.

At the top is the header section, which shows the OC://WebConnect Pro version accessed and the name of the HTML page displayed, **Server Configuration**, in the upper right corner.

On the left are navigation buttons to access other OC://WebConnect Pro HTML pages for configuration Server IP address, ports, security features, and administrator password.

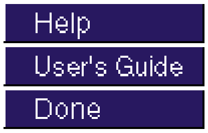
To the middle and right is the configuration section to make server configuration choices and enter server configuration data.

Navigation Buttons

Services – Enter the IP address and port for the JCP, Secure JCP, and Administration HTTP and HTTPS services. JCP is the service for non-SSL emulation sessions. Secure JCP is the service for emulation sessions secured by SSL. The Admin service is for the CGI-BIN connections used to query the server for current server and session information.

Security – Enable client token authentication, suppress host information, set the SSL cipher suite, and set the adminstrator password.

Misc – Set the OC://WebConnect Pro license key and enable JCP Client Are You There.



Access context-sensitive help.

Access the online user guide.

Exit the server configuration pages.

Setting Server IP Addresses and Ports

1. From the **Start Sessions** HTML page, select **Configuration**.
2. Type the administrator password and click **OK**. The **Configuration** page is displayed.
3. Choose the **Servers** button on the left. The **Configuration Servers** page is displayed.
4. Select the server to configure and click **Edit**. The **Server Configuration** page is displayed.
5. Type the IP address for each service.

   Each OC://WebConnect Pro 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 Pro servers to respond to requests from all installed network interfaces. Specify another IP address to limit OC://WebConnect Pro to one network interface.
6. Input the port number for each service.

   OC://WebConnect Pro emulation server can use up to three ports during operation. The default port setting can be used, or a different port number greater than 0 or less than 65,535 can be specified. Root privileges are required to use a port number less than 1024. A port number of 0 disables a port.
7. Click **Save**. For the changes to take effect, restart the OC://WebConnect Pro server. HTML files used to access OC://WebConnect Pro will have to be updated. Use the OC://WebConnect Pro configuration utility to update these files or manually edit the HTML files.

Setting Server Security Options

1. On the **Start Sessions** HTML page, select **Configuration** on the left side of the window .
2. Type the administrator password and click **OK**. The **Configuration** page is displayed.
3. Click **Servers** on the left. The **Configuration Servers** page is displayed.
4. Select the server to configure and click **Edit**. The **Server Configuration** page is displayed.
5. Click **Security** on the left side of the window. The **Security** page is displayed.
6. Make the necessary security changes. The following table describes the fields on this panel.

Field	Description
Suppress host information	By default, emulation windows display the DNS host name or address of the host accessed by the OC://WebConnect Pro client. Set this option to prevent this information from displaying on the title bar or in the help desk information.
Require HTTPS client authentication	Set this option to require a valid X.509 client certificate from the browser to establish a secure HTTP session with the Web server using SSL. This setting, in addition to the token authentication described below, ensures that only authorized users can access your system. **Note:** The Web server must be configured with the certificate or certificates of the CA(s) that issued the client certificates. See “Client Authentication.”
Use token authentication	Set this option to provide secure authentication between a browser-based client and the OC://WebConnect Pro server. When this option is set, a token is passed from the OC://WebConnect Pro server to the applet via an applet parameter and then passed back to the OC://WebConnect Pro server when an emulation session is established. This guarantees that the client establishing the connection was previously authenticated by the server via X.509 certificates or another client authentication scheme before the applet was downloaded, and that the applet parameters were not altered somewhere in between. The timeout value is a number in seconds in which the client must connect to the OC://WebConnect Pro server. When the timeout value lapses, the applet sets a connection refused, and another applet will have to be started with a new token to successfully connect.

Field	Description
Allow host resource override	Set this option to allow an applet to override certain parameters in the selected session file. The override values are passed to the applet as parameters when the applet tag is downloaded from the Web server. *Required* if **Access Control** (described below) is set to **Optional** or **Required**.
Access Control	The access control functions let you override default session parameters by user ID. They can be used to connect users to specific LUs. Select from these options: **None** – Default. Disables access control. **Optional** – Lets the administrator set up access control as needed. **Required** – Requires access control to be set for all sessions. When **Optional** or **Required** is selected, the administrator can set user access control. See “Controlling Session Access” in this chapter.
Administration Password	To change the administrator password, type the new password in this field. The administration password restricts access to the configuration screen to authorized users.
Confirm Password	Retype the password typed in **Administration Password** to verify the password was typed correctly.
GUI Config Cipher Suite	Check this option to select an SSL cipher suite to encrypt configuration sessions between the GUI Configurator applet and the OC://WebConnect Pro server.

7. Click **Save** to save the changes.

Setting the License Key

1. Select the **Configuration** button from the **Start Sessions** HTML page.
2. Enter the administrator password and click **OK**. The **Configuration** page is displayed.
3. Choose the **Servers** button on the left. The **Configuration Servers** page is displayed.
4. Select the server to configure and press the **Edit** button. The **Server Configuration** page is displayed.
5. Choose the **Misc** button. The input box for the license key is displayed with the current key.
6. Type the new license key and click **Save.**

OC://WebConnect Pro GUI Configuration

The OC://WebConnect Pro GUI Configurator utility is a JDK 1.1 Java applet accessed via a JDK 1.1 Java-enabled browser. The OC://WebConnect Pro emulation server must be running to use these tools. Using this Java applet, you can remotely configure the following options:

- Modify the OC://WebConnect Pro emulation server ports.
- Modify OC://WebConnect Pro administration ports.
- Select Cipher suites.
- Set **Allow User Configuration** to allow users to configure their own user interface features such as keyboard map and color map.
- Configure to conceal host connection information from client emulation users.
- Enable and configure Client Token authentication.
- Configure Client **Are You There?**
- Modify the administration password.
- Modify the server license key.
- Restart OC://WebConnect Pro emulation server.
- Enable OC://WebConnect Pro tracing.
- Shut down OC://WebConnect Pro emulation server.
- Kill individual emulation sessions.
- Create, delete, or modify all features of all session configurations including mapping keyboards, colors, attributes.

After the OC://WebConnect Pro server (see *Chapter 2: Starting OC://WebConnect Pro)* starts, the GUI Configurator applet can be accessed by selecting the Administration button on any OC://WebConnect Pro HTML page using a JDK1.1 Java-enabled browser.

☞

More Information

The Administration button can be removed from any of the OC://WebConnect Pro HTML pages or custom HTML may be written to access the GUI configuration applet. See *Chapter 12: Customizing OC://WebConnect Pro* for more information.

The GUI Configuration applet can be started in one of two modes, User mode or Administrative mode, depending on the **Allow User Configuration** option explained in detail below. Briefly, **Administrative mode** means **Allow User Configuration** *is **not** enabled*, the GUI Configuration applet is password protected, and if the correct password is entered the full GUI Configuration utility will be started. **User mode** means the **Allow User Configuration** is *enabled*, the user is not prompted for a password, the GUI Configuration for end user will be displayed, and all changes are written to the browser platform, not the server. The **Administrative mode** is accessible through the **User Mode** but is protected by password.

Logging On as Administrator

After the GUI Configurator applet has been downloaded to the browser the **Configuration Permissions Dialog** window displays asking for the Administrator password.

1. Type the appropriate password in the **Administrator Password** field.
2. Choose the **OK** button. The OC://WebConnect Pro **GUI Configurator** window displays in Administrative mode.

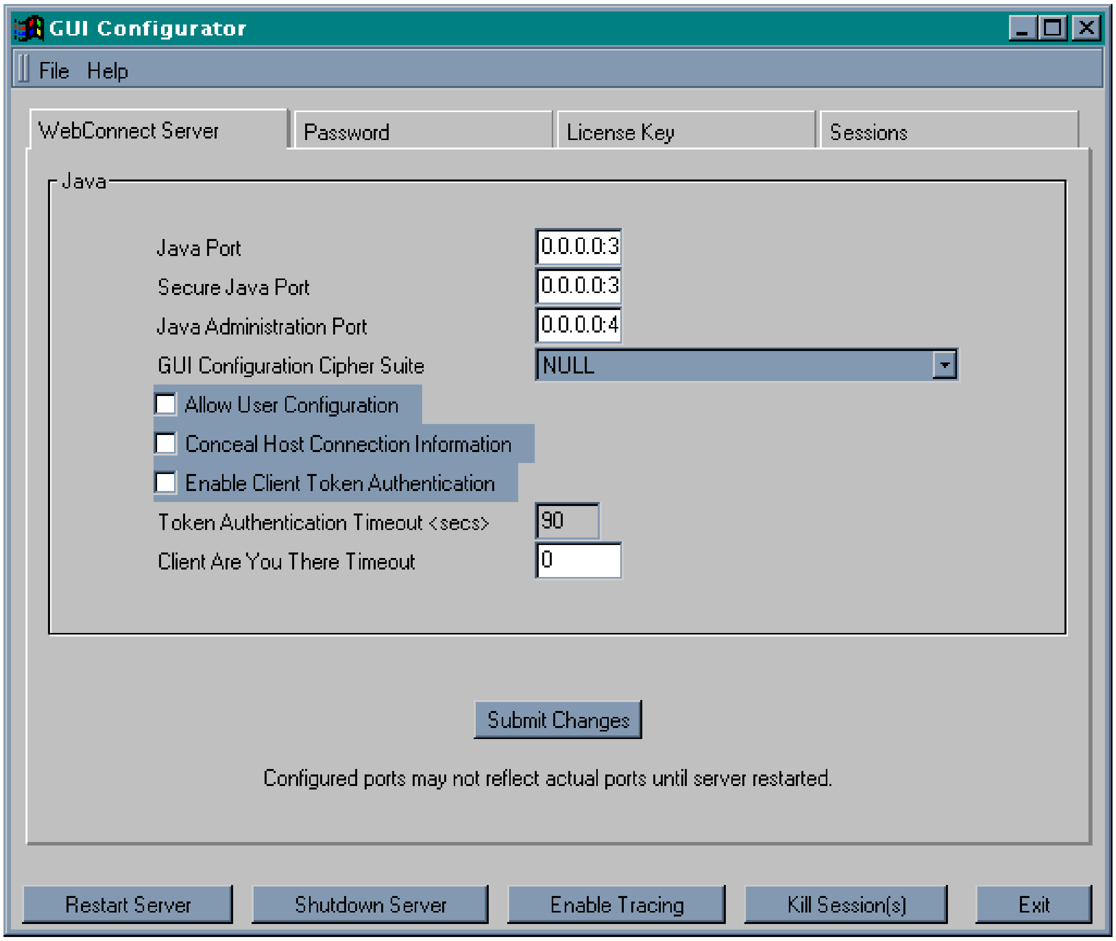
   -or-

   Click **Cancel** to return focus to the main OC://WebConnect Pro HTML page.
3. When the correct Administrator password is entered, the GUI Configurator applet appear with the current configuration information including four tabs:

   - OC://WebConnect Pro server
   - Password
   - License Key
   - Sessions

Using the WebConnect Server Tab

The WebConnect Pro **Server** tab is available only in administrative mode. Use this tab to configure server ports and to enable Secure Socket Layer (SSL) protocol for the server.



Java Port 0.0.0.0:3

Secure Java Port 0.0.0.0:3

Java Administration Port 0.0.0.0:4

GUI Configuration Cipher Suite NULL

□ Allow User Configuration

□ Conceal Host Connection Information

□ Enable Client Token Authentication

Token Authentication Timeout <secs> 90

Client Are You There Timeout 0

Configured ports may not reflect actual ports until server restarted.

Changing Server Configuration

1. Make the desired change in the OC://WebConnect Pro server configuration. Each configuration option is discussed in more detail below.
2. Save changes to the OC://WebConnect Pro server by selecting the **Submit Changes** button. A write successful dialog appears to indicate the changes were made.

Some changes made to the OC://WebConnect Pro server require the OC://WebConnect Pro server to be restarted for the changes to take effect. Use the **Restart Server** button to apply the new settings.

The settings that require the OC://WebConnect Pro server to be restarted include **Java Port** IP Address and port, **Secure Java Port** IP Address and port, and **Java Administration Port** IP Address and Port.

Configuring Server Ports

The OC://WebConnect Pro server uses three ports during operation, one for each service as shown below.

Default Settings

IP Address and Port Number	Service	Description
0.0.0.0:3270	Java Server	Listening port for use by non-SSL Java emulation clients. *Required*.
0.0.0.0:3443	Secure Java Server	Listening port for use by SSL Java emulation and administration clients. *Optional* if not using SSL.
0.0.0.0:4270	Java Administration	Listening port for use by the 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.

Server IP Addresses and Ports

Each OC://WebConnect Pro 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, will cause OC://WebConnect Pro servers to respond to requests from all installed network interfaces. Specify another IP address to limit OC://WebConnect Pro to one network interface.

OC://WebConnect Pro emulation server can use up to three ports during operation. The default port setting may be used or enter a port number greater than 0 or less than 65,535. Root privileges are required to use a port number less than 1024. A port number of 0 will disable a port.

Specify the Server IP Address and Port number in the following format:

ip address:*port number*

Example: 0.0.0.0:2080

For the changes to take effect, restart the OC://WebConnect Pro server. HTML files used to access OC://WebConnect Pro will have to be updated. Use the OC://WebConnect Pro configuration utility to update these files or manually edit the HTML files.

Configuring GUI Configuration Cipher Suite

To use SSL for the connection between the OC://WebConnect Pro server and the GUI Configurator applet, select a cipher suite from the **GUI Configuration Cipher Suite** list box. Cipher Suites specify the algorithms to be used for authentication, data encryption, data compression, and verification of message integrity when normal session traffic begins. If NULL is selected for the cipher suite, the GUI Configuration applet will use the non-SSL port to connect to the OC://WebConnect Pro server.

☞

More Information

SSL and GUI Configuration Cipher Suites are explained in more detail in *Chapter 15: Security Overview*.

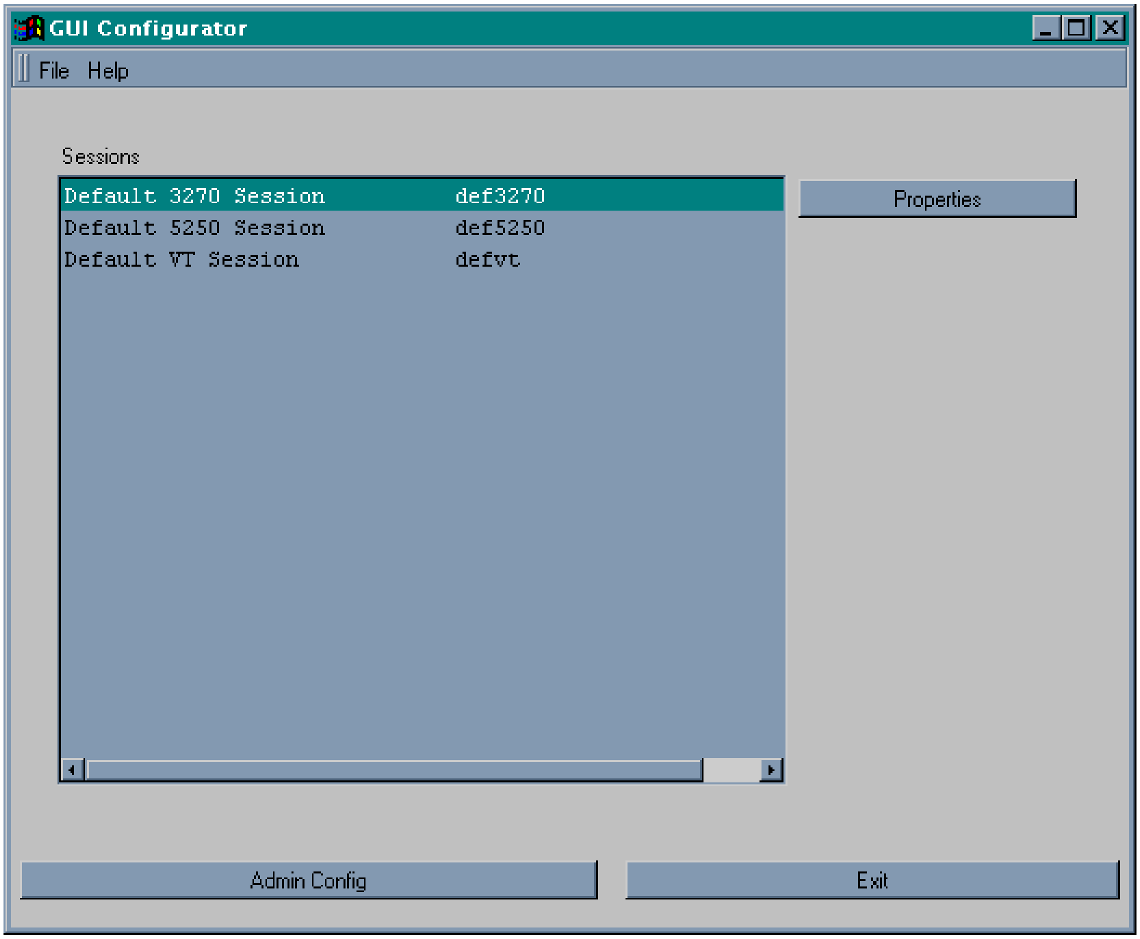
Concealing Host Connection Information

Enable **Conceal Host Connection Information** to prevent the display of the host name, IP address, and port number of the configured and connected TN server or UNIX system within the emulation client sessions. By default, this information is displayed under the Help Desk menu option on all emulation client interfaces. Submit changes.

Allowing User Configuration

Enable the **Allow User Configuration** check box to allow “end users” or those users of OC://WebConnect Pro who do not have administrative access to be able to configure the Client Interface Settings for each type of emulation client interface. The end user will be allowed to configure their own personal keyboard map, color map, attribute map, hot spot map, and Auto GUI map for each type of emulation: 3270, 5250, and VT. These maps will be based off the default maps configured with the server but will not affect the maps on the server because the maps are stored in the **WebConnect** directory in the browser HOME directory of the browser system. For example, a user 3270 emulation keyboard map file would be **userdef3270.kbm**.

User configuration files are used when a Emulation client applet is downloaded and started on the browser system. A search is made of the browser system to find any end user configuration files. If a file is found that keyboard map or color map, etc. overlays the map downloaded from the server.



Default 3270 Session	def3270
Default 5250 Session	def5250
Default VT Session	defvt

Enabling Client Token Authentication

Enable the Client Token Authentication option to use the OC://WebConnect Pro option which uses a token to verify that the emulation client applet connecting the OC://WebConnect Pro server is genuine.

Token Authentication Timeout <sec>

Specify, in seconds, the amount of time to wait for token authentication before a Client connection is rejected by the OC://WebConnect Pro server.

A token is issued when an emulation session applet is initiated. The time out value is the amount of time allowed after the token is issued and before it is used for session startup. If the time out value is exceeded a host connect will not be allowed. This safeguards against a token value being stolen and used at a later time to gain host access.

☞

More Information

Client Token Authentication is explained in more detail in *Chapter 15: Security Overview*.

Client Are You There Timeout

Enable the **Client Are You There Timeout** option to prompt the server to conduct an "are you there" check to determine if a session is active. If not active, the server closes down the session between the Java client and the OC://WebConnect Pro server. The timeout value is in minutes. Specify **0** to disable the option.

Using the Password Tab

Use the Password tab on the OC://WebConnect Pro **GUI Configurator** window to set the administrator password. This password is used to allow access to this GUI Configurator and HTML configuration pages.

1. Select the **Password** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Type the new administrator password in the **Set Password** field. (The default password is **OCS**.) It is recommended that the administrator password be changed from the default.
3. Type the password again in the **Confirm** field. Each character displays as an asterisk as it is entered.
4. Submit the password change by selecting the **Set Password** button.

☞

Note: If the passwords in both boxes are not identical, both boxes clear when the Set Password button is used.

Using the License Key Tab

The OC://WebConnect Pro license key is used to license the OC://WebConnect Pro server for the number of concurrent sessions and server expiration. Use the **License Key** tab to set the license key.

1. Select the **License** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Enter the authorized license key in the **License Key** field.
3. Press the **Set Key** button.

Using the Sessions Tab

Use the **Sessions** tab on the OC://WebConnect Pro **GUI Configurator** window to

- Create session configurations.
- Delete session configurations.
- View and modify session properties.

The **Sessions** tab displays a list of defined sessions, a **Create** button, a **Delete** button, and a **Properties** button. Use the **Create** button to create a new session. The **Delete** button allows administrators to delete a defined session. The **Properties** button displays a configuration window that allows the properties and associated map files for a selected session to viewed or modified.

More Information

For more information about Session configuration creation, deletion, or modification refer to one of the following chapters within this document:

- *Chapter 6: 3270 Session Configuration and Features*
- *Chapter 7: 5250 Session Configuration and Features*
- *Chapter 8: 3287 Print Session Configuration and Features*
- *Chapter 9: VT Session Configuration and Features*

Using Administration Tab Buttons

Restarting Server Ports

1. Select the **WebConnect Server** tab on the **GUI Configurator** window.
2. Select the **Restart Server** button to restart the OC://WebConnect Pro server ports and confirm restart.

Caution

All active Java client sessions will be killed!

Enabling Tracing

1. Select the **OC://WebConnect Server** tab on the GUI Configurator window.
2. Select the **Enable Tracing** button. The **Start Trace** dialog window displays.
3. Type a **.trc* trace filename in the **Filename** box in the fourth quadrant. Do not use an extension.
4. Type a brief description or reason for the trace in the **Reason** box.
5. Use the **Start Tracing** button to begin recording communication information exchanged between the OC://WebConnect Pro server, the host, and the Java client.
6. Trace files are stored in the OC://WebConnect Pro directory in the **logs** directory (default is **wc/logs**).

> **Note:** The Start Tracing button toggles to Stop Tracing when tracing begins. Tracing remains on for all sessions until disabled.

Shutting Down the Server

Use the **Shutdown Server** button to shut down the OC://WebConnect Pro server and confirm shutdown.

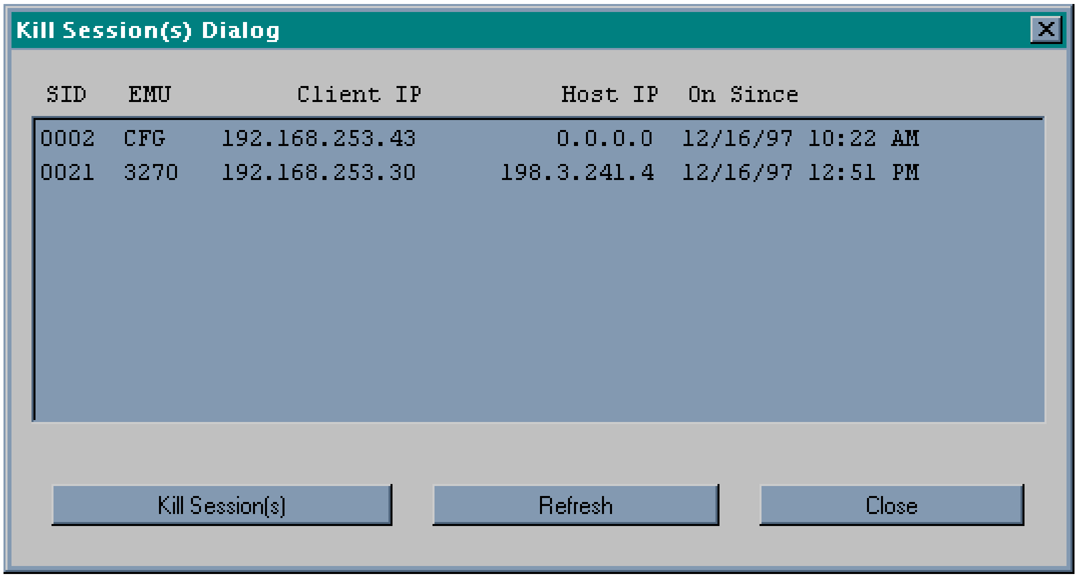
> **Caution**
>
> All active clients will be killed! The OC://WebConnect Pro emulation server will have to be started from a UNIX command prompt or the NT services panel.

Killing a Session

A hung session or multiple sessions can be terminated at the administration level by using the **Kill Session** button on the **GUI Configurator** window. The terminated session displays with a red line at the administration and client levels.

To kill a session or multiple sessions:

1. Use the **Kill Session** button on the **GUI Configurator** window from administrator mode. The **Kill Session (s) Dialog** displays.



SID	EMU	Client IP	Host IP	On Since
0002	CFG	192.168.253.43	0.0.0.0	12/16/97 10:22 AM
0021	3270	192.168.253.30	198.3.241.4	12/16/97 12:51 PM

2. Select the session or sessions to terminate.

3. Select the **Kill Session** button on the **Kill Session Dialog** window. OC://WebConnect Pro disconnects the sessions selected. The list of sessions is a snapshot of the sessions connected. The **Refresh** button updates the list of open sessions if there have been any connections or disconnects since the dialog was displayed.

Server Ports

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 traffic (Web traffic).

OC://WebConnect Pro allows five possible ports and requires at least two ports:

- At least one Java server port or one secure Java server port is required.
- If not using a third-party HTTP server, at least one HTTP server port or one HTTPS server port is required.

The OC://WebConnect Pro ports are described in the following table.

IP Address and Port Number	Service	Description
0.0.0.0:3270	Java Server	Listening port for use by non-SSL Java emulation clients.
0.0.0.0:3443	Secure Java Server	Listening port for use by SSL Java emulation and administration clients.
0.0.0.0:4270	Java Administration	Listening port for use by the 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, selecting sessions, and downloading client applets.
0.0.0.0:2443	HTTPS Server	SSL-protected HTTP server.

Chapter 6: Configuring 3270 Emulation Sessions

Overview

OC://WebConnect Pro combines a feature-rich, 3270-emulation client with centralized configuration and administration on the server.

3270 emulation features include 3270E, 3278 and 3279 terminal types, Models 2 – 5; 3287 Print; and IND$File transfer. Client interface features include keyboard, color, and attribute mapping; copy and paste; and screen print. All emulation sessions can be protected by either RSA's RC4 encryption or SSL authentication and encryption.

Session configuration is provided via centralized configuration and administration tools that can be accessed remotely through a browser. OC://WebConnect Pro provides two methods to configure OC://WebConnect Pro emulation sessions:

- The HTML configuration is a series of HTML pages that access the OC://WebConnect Pro server via a common gateway interface (CGI) interface to create, modify, and delete emulation session configurations via a browser. The HTML configuration does not require a Java-enabled browser.
- The graphical **GUI Configurator** is a Java applet downloaded to the browser platform and executed via a Java-enabled (JDK 1.1) browser.

Both configuration tools provide full-featured, remote session configuration to create, delete, and modify emulation sessions. An OC://WebConnect Pro server administrator can control important session configuration and management features like host access, security, session negotiation rules, and emulation interface configuration. If desired, the end user can be allowed to configure the keyboard, color, and attribute mapping.

Configuring 3270 Sessions Using HTML

The OC://WebConnect Pro HTML configuration is a series of HTML pages that retrieve the current server and session information from the OC://WebConnect Pro server through an administrative connection. An administrator can modify server settings and create, modify, or delete emulation session settings. The OC://WebConnect Pro server must be active to use the HTML configuration utility. See *Chapter 2: Starting OC://WebConnect Pro.*

Accessing the 3270 HTML Session Configuration Page

1. Connect to the OC://WebConnect Pro HTTP Web server: In the URL of a browser, type the following:

   - The host name where the OC://WebConnect Pro HTTP Web server is running
   - The TCP port number

   Example:

   http://host1.oc.com:2080

2. Press **Enter**. The **Start Sessions** page is displayed.

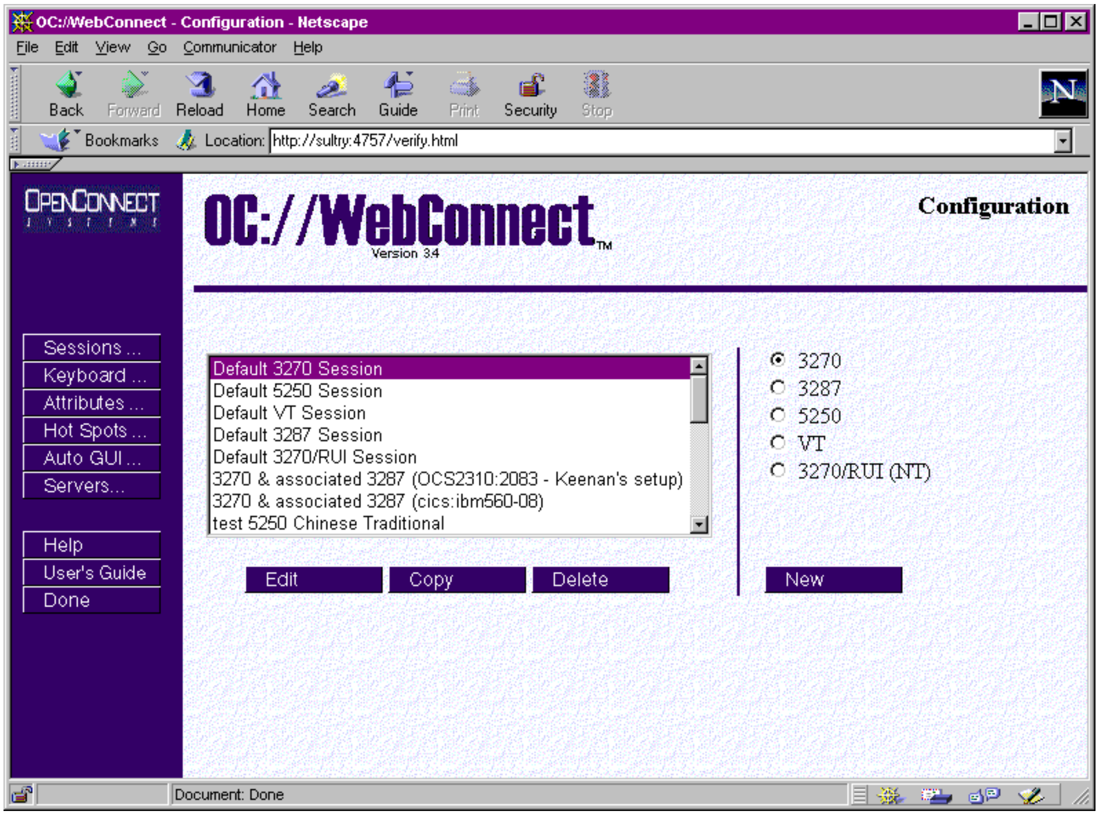
3. Click **Configuration** on the left of the **Start Sessions** page. A prompt appears for the **Administrator Password.**

4. Type the password in the box under **Enter Administrator Password** and click **OK**.

☞

Note: The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

When the correct administrator password is entered, the main **Configuration** HTML page is displayed.



Location: http://sultry:4757/verify.html

OC://WebConnect™ Version 3.4

Configuration

Default 3270 Session
Default 5250 Session
Default VT Session
Default 3287 Session
Default 3270/RUI Session
3270 & associated 3287 (OCS2310:2083 - Keenan's setup)
3270 & associated 3287 (cics:ibm560-08)
test 5250 Chinese Traditional

● 3270
○ 3287
○ 5250
○ VT
○ 3270/RUI (NT)

Document: Done

The main **Configuration** page has three sections:

- At the top is the header section, which shows the OC://WebConnect Pro version and the name of the HTML page displayed, **Configuration** in this example.

- On the left are navigation buttons used to access other OC://WebConnect Pro HTML pages for context-sensitive **Help**, the online **User’s Guide**, and configuration pages for mapping other OC://WebConnect Pro features. The **Done** button exits this page.

- To the middle and right is the session configuration section used to create, edit, or delete session configurations.

Navigation Buttons

Sessions – Configure an individual session configuration. This page is displayed first.

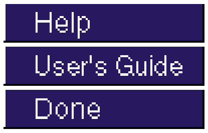
Keyboard – Create, modify, or delete a keyboard map.

Attributes – Create, modify, or delete an attribute and color map.

Hot Spots – Create, modify, or delete a hot spot map.

Auto GUI – Create, modify, or delete an auto GUI map.

Servers – Modify server settings.



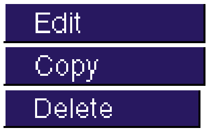
Access context-sensitive help.

Access online user guide.

Exit session configuration.

Session Configuration Buttons

A list of existing session configurations is displayed. To edit, copy, or delete an existing session, select a session and click the appropriate button.



Edit an existing session configuration.

Create a new session configuration from an existing session configuration.

Delete an existing session configuration.

A group of radio buttons indicates the supported emulation types. To create a new session configuration, choose an emulation type, and then click **New**.

Create a new session configuration.

Configuring a New 3270 or 3270/RUI Session with HTML

1. Click the **3270** or **3270/RUI (NT)** radio button.
2. Click **New**. A new session configuration page, **Description**, appears with the *default* session settings.
3. Type a unique session description and filename (without an extension).
4. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **3270**, **3287**, **Display**, **Printing**, and **Scripting**. Modify the settings as needed.

☞

More Information

For more information about 3270 emulation features, see “3270 Emulation Session Features and Settings” in this chapter.

5. To save the new 3270 or 3270/RUI session configuration, click **Save** on the sidebar.

   -or-

   To abort the creation of a new 3270 or 3270/RUI session configuration, click **Cancel** on the sidebar.

Editing an Existing 3270 or 3270/RUI Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Edit**. The first session configuration page appears with the chosen session description.
3. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **3270**, **3287**, **Display**, **Printing**, and **Scripting**. Modify the settings as needed.

☞

More Information

For more information about 3270 emulation features, see “3270 Emulation Session Features and Settings” in this chapter.

4. To save the changes, click **Save** on the sidebar.

   -or-

   To cancel the changes made to an existing 3270 or 3270/RUI session configuration, click **Cancel** on the sidebar.

Copying an Existing 3270 or 3270/RUI Session Configuration Using HTML

1. Select an existing session configuration.

2. Click **Copy**. A new session configuration page appears with the same session settings.

3. Type a unique session description and file name.

4. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **3270**, **3287**, **Display**, **Printing**, and **Scripting**. Modify the settings as needed.

☞

> **More Information**
>
> For more information about 3270 emulation features, see “3270 Emulation Session Features and Settings” in this chapter.

5. To save the new 3270 or 3270/RUI session configuration, click **Save** on the sidebar.

   -or-

   To cancel the creation of a new 3270 or 3270/RUI session configuration, click **Cancel** on the sidebar.

Deleting an Existing 3270 or 3270/RUI Session Configuration Using HTML

1. Select an existing session configuration.

2. Click **Delete**. A new page appears requesting you to confirm the deletion.

3. Click **Delete** again to delete the selected session.

   -or-

   Click **Cancel** to stop the deletion.

☞

> **Note:** Default session configurations cannot be deleted.

Configuring 3270 Sessions Using the GUI Configurator

After the OC://WebConnect Pro server is started (see *Chapter 2: Starting OC://WebConnect Pro*), you can access the GUI Configurator applet by selecting **GUI Config** on any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser.

☞

More Information

You can restrict access to the GUI Configurator applet by removing the button from any OC://WebConnect Pro HTML page, or you can create custom HTML access to the GUI Configurator applet. See *Chapter 12: Customizing OC://WebConnect Pro*.

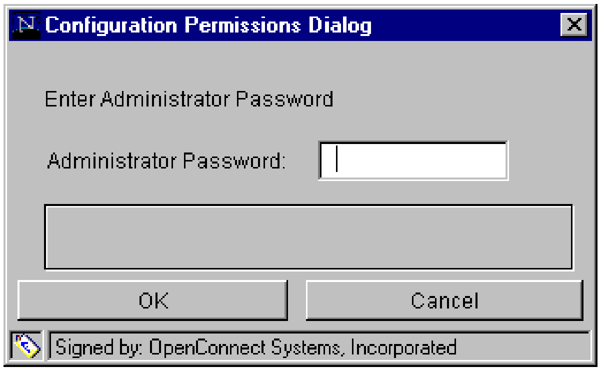
Accessing the GUI Configurator for 3270 Session Configuration

1. Start the OC://WebConnect Pro server. (See *Chapter 2: Starting OC://WebConnect Pro*.)

2. From any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser, click **GUI Config** on the sidebar. The browser downloads and starts the GUI Configurator applet.

   You might see one or more Java permissions windows. Click **Grant** in each window to authorize the applet to run.

   After the applet starts, the **Configuration Permissions Dialog** window displays asking for the administrator password.



Configuration Permissions Dialog

Enter Administrator Password

Administrator Password:

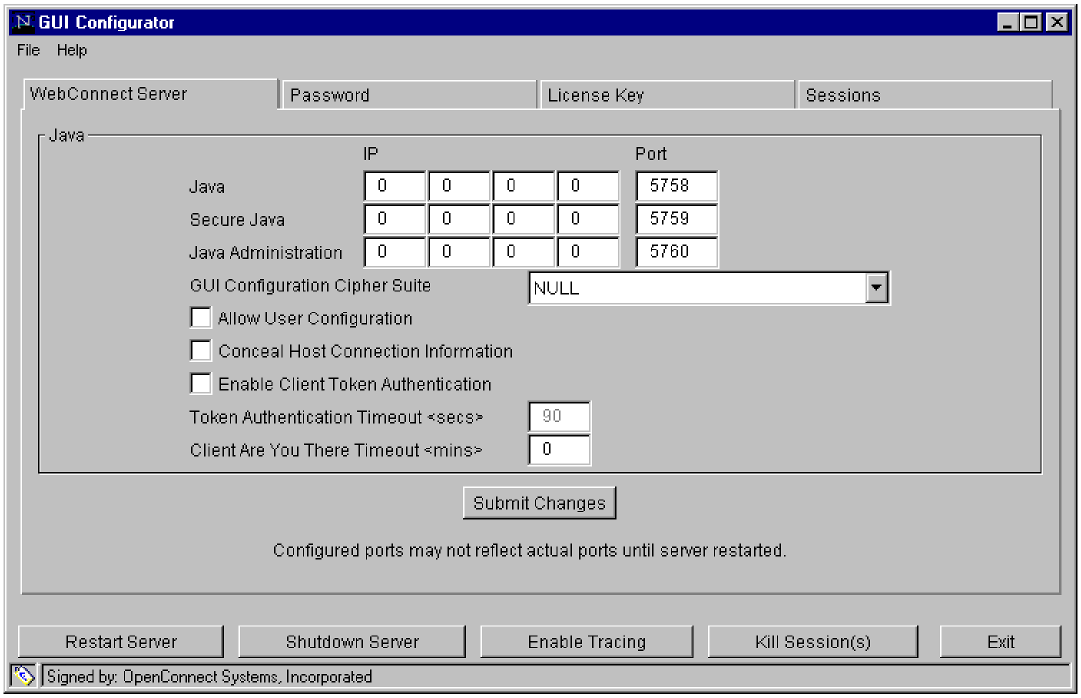
Signed by: OpenConnect Systems, Incorporated

3. Type the password in the **Administrator Password** field and click **OK**.

☞

Note: The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

When the correct administrator password is entered, the OC://WebConnect Pro **GUI Configurator** window, shown below, opens:



	IP				Port
Java	0	0	0	0	5758
Secure Java	0	0	0	0	5759
Java Administration	0	0	0	0	5760

GUI Configuration Cipher Suite NULL

□ Allow User Configuration

□ Conceal Host Connection Information

□ Enable Client Token Authentication

Token Authentication Timeout <secs> 90

Client Are You There Timeout <mins> 0

Configured ports may not reflect actual ports until server restarted.

Signed by: OpenConnect Systems, Incorporated

The window has four tabs at the top. The tab currently selected is OC://WebConnect Pro **Server**.

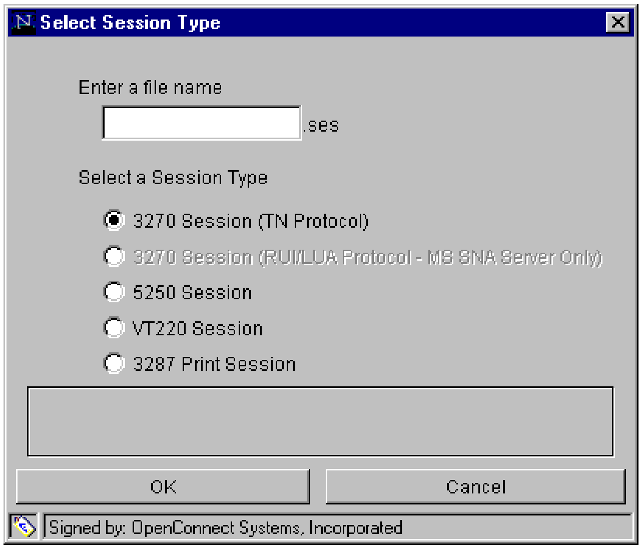
More Information

For more information on the OC://WebConnect Pro **Server**, **Password**, and **License Key** tabs, see *Chapter 5: Server Configuration and Administration*.

Configuring a New 3270 or 3270/RUI Emulation Session

1. Click the **Sessions** tab on the OC://WebConnect Pro **GUI Configurator** window. A list of defined sessions displays.

2. Click **Create**. The **Select Session Type** window displays.



Select Session Type

Enter a file name

[ ] .ses

Select a Session Type

● 3270 Session (TN Protocol)

○ 3270 Session (RUI/LUA Protocol - MS SNA Server Only)

○ 5250 Session

○ VT220 Session

○ 3287 Print Session

OK | Cancel

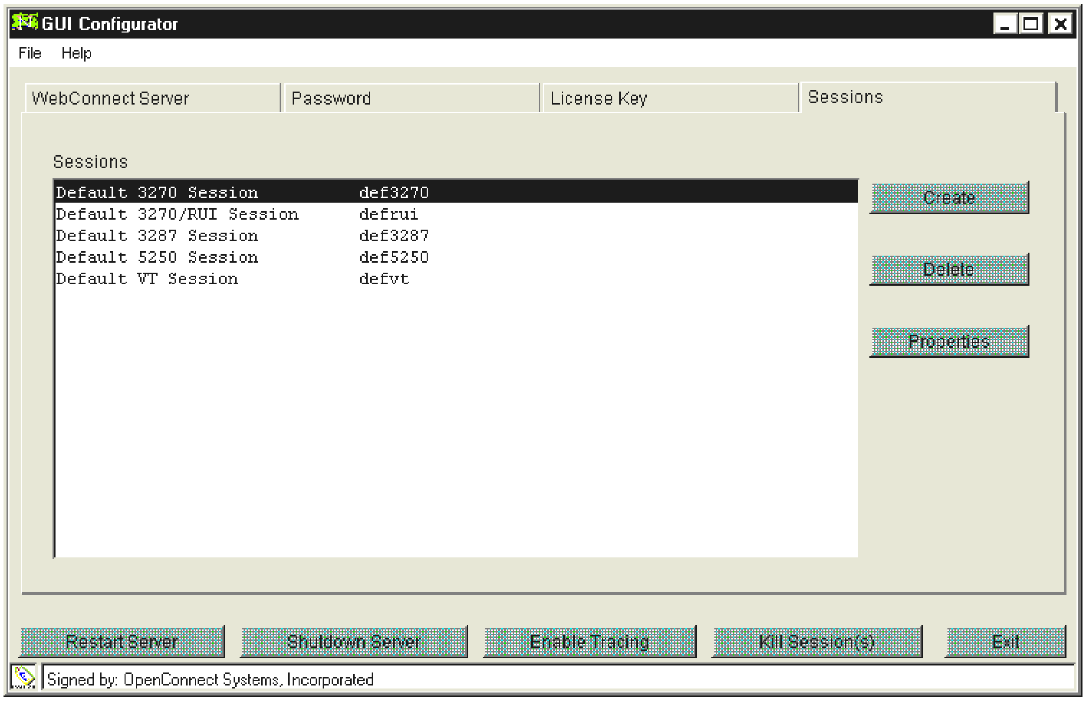
Signed by: OpenConnect Systems, Incorporated

3. Type a unique file name (without an extension) for the new session.

Notes

- When choosing a file name for a session configuration, consider that files are listed on the **Sessions** window in alphabetical order.
- To restore the form to default display values, select the **Defaults** button.

4. Select **3270 Session (TN Protocol)** and click **OK**. The **GUI Configurator** displays the **Session Properties** window for the selected emulator type.



```
Default 3270 Session          def3270
Default 3270/RUI Session      defrui
Default 3287 Session          def3287
Default 5250 Session          def5250
Default VT Session            defvt
```

Signed by: OpenConnect Systems, Incorporated

5. Modify **Session Settings** options as needed on the **Session Properties** window.

6. Click each radio button and modify settings if necessary:

   - **Display Settings**
   - **3270 Settings**
   - **TN Protocol Settings**
   - **Print Settings**

7. Now, step through the other tabs—**Auto GUI**, **HotSpots**, **Attributes**, **Color**, and **Keyboard**—modifying settings as needed. Each configuration option is discussed in “3270 Emulation Session Features and Settings” in this chapter.

> **Note:** The tabs displayed depend on the mode the configuration applet is in and the emulation type of the session selected. For example, if the applet is in user mode, the **Sessions Properties** tab does not display.

8. Click **OK** to save the session configuration to a session (***.ses**) file.

   -or-

   Click **Cancel** to abort creating the new session.

Editing a 3270 or 3270/RUI Session Configuration

1. Click the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to edit and click **Properties**. The **GUI Configurator** displays the **Session Properties** window for the selected emulation type.
3. Modify **Session Settings** options as needed on the **Session Properties** window.
4. Click each radio button and modify settings if necessary:
   - **Display Settings**
   - **3270 Settings**
   - **TN Protocol Settings**
   - **Print Settings**
5. Now, step through the other tabs—**Auto GUI**, **HotSpots**, **Attributes**, **Color**, and **Keyboard**—modifying settings as needed.

☞ **More Information**

For more information about 3270 emulation features, see “3270 Emulation Session Features and Settings” in this chapter.

6. Click **OK** to save the session configuration to a session (***.ses**) file.

   -or-

   Click **Cancel** to abort saving the changes.

Deleting a 3270 or 3270/RUI Emulation Session Configuration

1. Choose the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to delete and click **Delete**. A window is displayed requesting confirmation of the delete.
3. Click **OK** to confirm the deletion. The session file is deleted.

☞ **Note:** Default session files cannot be deleted.

3270 Emulation Session Features and Settings

Description

Field	Procedure
Description	Type a brief description for the session configuration. This description appears on windows used to select a session to start, modify, or delete.
Save as	Type a unique file name, without an extension, in which to store the emulation session settings.

3270 Network Settings

Field	Procedure
Connect to host	Enter the host name of the destination system. This can be the TCP/IP host name of the mainframe system or of a gateway that provides TCP/IP services to the mainframe system.
Port	Enter the TCP/IP port number of the gateway or TN server used for emulation connections. The default Telnet port number is **23**.
Enable TCP/IP Keep Alive	Enable this option for OC://WebConnect Pro to utilize the Keep Alive feature of the underlying TCP/IP stack to monitor and clean up after unexpected session outages, such as PC client power losses or cable faults. Keep Alive monitors the connection from the browser client to the OC://WebConnect Pro server, as well as the connection from the OC://WebConnect Pro server to the TN3270 server.
Try Multiple IP addresses	Enable this option if the host name being used for host connectivity refers to multiple DNS addresses. Multiple DNS addresses provide the OC://WebConnect Pro server a choice of gateways or TN servers when a server is busy or the session type is not available. **Note:** If this option is not enabled, only one connection attempt—to the first IP address returned—is made. OC://WebConnect Pro evaluates the DNS addresses serially to make a host connection, depending on the TN Server or gateway used. • If using an OC://WebConnect Pro SNA Access Server Gateway, evaluation is based on the availability of the specified model and LU type, a specific LU name, a specific LU number, and/or access to a specific SAC LU Pool. • If using a TN3270E server, evaluation is based on the model and LU type or a specific LU name

Field	Procedure
	• If using a general TN server, evaluation is based on the model and/or LU type. Example: Host XY is configured for two IP addresses (gateway X and gateway Y). OC://WebConnect Pro wants a 3279 LU, and all 3279 LUs on gateway X are in use. OC://WebConnect Pro automatically attempts to connect to a 3279 LU on gateway Y.
Use virtual gateway	Enable this option to instruct OC://WebConnect Pro to access an OpenConnect Systems virtual gateway to the host gateway for this client location. This option requires an SNA Access Server Gateway.
Enable data compression	Enable this option to compress data flowing between the OC://WebConnect Pro server and the Java client. **Note:** The tradeoff for decreased network traffic is time spent compressing and decompressing data.

3270/RUI Network Settings

Field	Procedure
LU Pool Name	Enter the LU or LU pool name of the NT SNA server to which this session will connect.
LU Type	Check the appropriate box to indicate whether this is a 3270 or LUA LU/POOL.
Enable data compression	Enable this option to compress data flowing between the OC://WebConnect Pro server and the Java client. **Note:** The tradeoff for decreased network traffic is time spent compressing and decompressing data.

Security Settings

Field	Procedure
Diffie-Hellman/RC4 encryption	Enable this option to encrypt session data between the OC://WebConnect Pro server and Java client session. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both.
Key Length	Select **40 bits** or **128 bits**. 128-bit encryption is available only in the US. If 128-bit encryption is selected for a non-US version, the session defaults to 40-bit encryption. The encryption method for a specific emulation can be seen by selecting **Help**>**Help Desk**. **Note:** Key length in Ultra Lite session is always **40 bits**.
SSL	Enable SSL (Secure Socket Layer) to use an SSL cipher suite for authentication and/or encryption of data between the OC://WebConnect Pro server and the Java client session. This option requires that the OC://WebConnect Pro server Secure Java Port is configured and active. See *Chapter 5: Server Configuration and Administration* for more information about the Secure Java Port. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both. Select **Optional** to allow emulation client users to choose SSL or not. Select **Required** to force the use of SSL session configuration.
SSL Cipher Suite	Select an SSL Cipher Suite based on the level of security desired.
Limit number of sessions per applet	Enable this option to restrict the number of new sessions that can be started from an emulation session already connected. Each Java emulation client has a **File**>**New** menu item, which allows a new emulation session to be spawned from the existing connection. By default, an emulation client user can start as many sessions as the OC://WebConnect Pro license key allows.
sessions per applet	Specify the number of sessions that can be spawned from an emulation applet. Zero disables this option.

☞

More Information

For more information about OC://WebConnect Pro security features, see *Chapter 15: Security Overview*.

Telnet Settings

Field	Procedure
Enable TN3270E	Check this box if the gateway or host TN server supports the enhanced TN3270 protocol, TN3270E. Enabling TN3270E allows the use of the Associate 3287 Printer feature.
Associate 3287 Printer	Select this feature to add a **File** menu option to the 3270 session emulation client, thus allowing a 3287 printer session to be started from a 3270 session. To utilize this feature, the gateway or host TN server must support the TN3270E Associate feature and must be set up with the desired display-to-printer association.
Telnet AYT -	Click the check box to instruct OC://WebConnect Pro to send "Are you there" messages to the host to maintain the connection between the OC://WebConnect Pro server and the gateway or Telnet server during periods of user or host inactivity. If this check box is not selected, messages are not sent to the host.
Idle Timeout minutes	Enter a value in whole minutes for OC://WebConnect Pro to wait for an AYT response from the remote host.
Terminal Type Demotion	Click the check box to allow OC://WebConnect Pro to sequentially negotiate model types below the alternate screen size. The negotiation continues until a model is selected for the session. -or- Uncheck the check box to allow normal default and alternate screen sizes to be negotiated between OC://WebConnect Pro and the gateway.
IP Pass Through	This parameter specifies whether IP pass through is enabled. • On – IP pass through is enabled and displays the negotiated IP address. • Off – IP pass through is not enabled. **Notes:** RTM support and IP pass through require an SNA Access Server Gateway version 3.8 or greater. Any other gateway must have IP pass through disabled. If the SNA Access Server Gateway has IP Health Check enabled, IP pass through is required, and RTM support is optional.
RTM Support	Click the check box to extend Response Time Monitoring (RTM) from the OC://WebConnect Pro server to the client. See notes above.
Device Names	Type one or more LU or Pool names of the OCS gateway, separated by a space.

3270 Settings

Field	Procedure
Device Type	Click the arrow to display the IBM device types that can be emulated in the session.
Monochrome	Click the check box to display session data in monochrome.
Default Screen Size	Click the arrow to display the IBM model type to be used for the default screen size (in the applet window for the session). • 2 – 24 rows by 80 columns • 3 – 32 rows by 80 columns • 4 – 43 rows by 80 columns • 5 – 27 rows by 132 columns
Alternate Screen Size	Click the down arrow to select the IBM model type to use for the alternate screen size (in the applet window for the session). See “Default Screen Size” for descriptions.
File Transfer Command	Enter the file transfer command to use for IND$FILE or APVUFILE transfers.
File Transfer Map Table	Select a default file transfer map file to use for IND$FILE or APVUFILE transfers.

3287 – TN3270E Associated Printer

Field	Procedure
Default Format Values	The default values described below can be overridden by commands in the data stream. The data stream can also issue commands that revert the session to default settings, causing these values to again take effect.
Characters Per Line	This setting corresponds to the MPP (Maximum Presentation Position) parameter defined for LU1 printing passed in the SHF (Set Horizontal Format) command. It also defines the end-of-line position for LU3 printing when the WCC printout format bits are set to 00. See **Wrap Lines Exceeding Line Length** below.
Lines Per Page	This setting corresponds to the MPL (Maximum Presentation Line) parameter defined for LU1 printing passed in the SVF (Set Vertical Format). The setting has no meaning in LU3 printing. See **Break Pages Exceeding Page Length** below.
Point Font Size	This setting corresponds to the LD (Line Density) parameter defined for LU1 printing passed in the SLD (Set Line Density) command. It also defines the font size used for LU3 printing when the **Auto Fit** option is disabled. If character mode is not enabled, the current value of LD is used directly as the font size and the line spacing is the default

Field	Procedure
	line spacing of the font. If character mode is enabled, the line spacing is computed as the Vertical Points Per Inch/Point Font Size. The font size is then chosen to fit the vertical and horizontal spacing.
Characters Per Inch	This setting, also know as character pitch, corresponds to the PD (Print Density) parameter defined for LU1 printing passed in the SPD (Set Print Density) command. It also defines the print density used for LU3 printing when the **Auto Fit** option is disabled. If this parameter is set to 0 and no SPD command is received in the data stream, or if character mode is not enabled, then the print output is printed in the default character spacing of the active font.
Auto Fit	Select this option to format the print output to fit the paper size. **Notes:** If this option is not enabled, the print font size is effectively fixed such that 80-column documents fit a portrait page setting, and 132-column documents fit a landscape page setting. In this mode, 132-column documents can overflow a portrait page. Setting AutoFit causes the 3287 applet to select a font for the current page setting, ensuring that lines are not truncated. The JavaScript print method does not support the Auto Fit feature.
Wrap Lines Exceeding Line Length	Setting this option causes the **Characters Per Line** setting to be honored, resulting in the automatic insertion of a New Line operation if an attempt is made to write beyond the right margin (as defined in the SHF command—*not* the margins set in the **Printing** settings for the session). This option is normally enabled. Disabling the option can be useful for applications to operate in raw mode and pass escape sequences through to the printer without risking the automatic insertion of a New Line character into the escape sequence.
Break Pages Exceeding Page Length	Setting this option causes the **Lines Per Page** setting to be honored, resulting in the automatic insertion of a Form Feed operation if an attempt is made to write beyond the current bottom margin (as defined in the SVF command—*not* the margins set in the **Printing** settings for the session). This option is normally enabled. Disabling this option can be useful for applications to operate in raw mode and pass escape sequences through to the printer without risking the automatic insertion of a Form Feed character into the escape sequence.

Display Settings

Field	Procedure
Language	Select the language to use for messages in the 3270 session emulation applet window.
Code Page	Enter the number of the code page for the target host application. Values range from 37 to 61712.
Transform Type	Select the code page transform type from the list box. **Note:** If using the Single/Double Byte EBCDIC-to-Unicode option, the ability to switch the single-byte code pages using a default key is available.
Font Size	Enter the number for the default font point size to use for text displayed in the applet window. This font size dictates the initial client window size.
Keyboard Map	Enter the keyboard map (**.kbm)** file name for the session being edited. The default is **def3270.kbm**.
Attribute Map	Enter the **.atm** file name for the session being edited. The default is **def3270.atm**.
Hot Spots	Enter the **.hsp** file name for the session being edited. The default is **def3270.hsp**.
Enable Auto GUI for this session.	Select this option to allow the emulation client user to toggle on or off the Auto GUI display option. If this option is disabled, the user does not have the Auto GUI option.
Auto GUI	Enter the **.agu** file name for the session being edited. The default is **def3270.agu**.
Clickpad	Enable this option to initially show a clickpad in an applet window. The clickpad can be used to select function keys or other special keys not mapped to the local keyboard.

☞

More Information

For more information about mapping user interface and display options, see *Chapter 10: Display Options Configuration and Features*.

Printing Settings

Field	Procedure
Radio buttons:	Select one.
Disabled	Select this option to disable screen print and 3287 printing for this 3270 session.
OC://WebPrint	Select this option to use OC://WebPrint (Windows platform only) for screen print and 3287 printing. OC://WebPrint must be installed on the browser platform to use this solution. This option is supported on JDK 1.0 and greater browsers. The OC://WebPrint print solution is available in all OC://WebConnect Pro applets and avoids some problems associated with JDK 1.1 printing by printing at the resolution of the underlying print driver. OC://WebPrint prints to any paper size reported by the printer driver and honors all session settings and formatting controls from the data stream, generating uniformly spaced print output. In addition, OC://WebPrint supports two features not supported by the other print solutions: • A raw mode of operation that allows printer-specific codes to be passed in the data stream. • A suppress-printer-dialog option to allow jobs to be sent directly to the default printer without user intervention.
JavaScript	Select this option to use JavaScript, which is supported in some JDK 1.0 and greater browsers. The JavaScript print solution is supported by all OC://WebConnect Pro emulation applets. JavaScript functions are downloaded to the PC as part of the HTML page that loads the emulation applet. Therefore, if you write an HTML page to load the applet, the page must include JavaScript print functions to prevent breaking the JavaScript print solution. When printing with the JavaScript print solution, the JavaScript opens a separate browser window, writes the print output to that window, and then sends the browser contents to the system printer as if the user selected **File**>**Print** from the browser menu. JavaScript printing is convenient and provides a good print solution for applications not requiring control of the output format. Because the print output is rendered through the browser, the browser is in charge of formatting, and virtually all session settings and data stream commands related to formatting are ignored.
JDK 1.1 Print	Select this option for screen print and 3287 printing using JDK 1.1 print methods embedded in JDK 1.1-based browsers. The JDK 1.1 print solution is the native print implementation provided by all browsers utilizing JDK 1.1 or later, making it available when

Field	Procedure
	using an Enhanced or Power User applet. The browser's JVM (Java Virtual Machine) implementing JDK 1.1 printing prints at a fixed resolution, typically 72 or 96 pixels per inch, which is usually less than the resolution of the attached printer. This mismatch causes incompatibilities with the **Windows Generic/Text Only** driver and can cause nonuniform character spacing when attempting to print at specified line and/or character densities. Printing with the **Auto Fit** feature enabled prevents the latter problem. **Note:** Screen printing always prints in **Auto Fit** mode. Early versions of JDK 1.1 implemented in most browsers contain bugs that affect the ability of OC://WebConnect Pro to properly determine the page size. In these older browsers, the page size is assumed to be 8.5-by-11-inch paper in portrait mode. As of JDK 1.1.4, most of these bugs have been fixed, allowing support of landscape mode and other paper sizes.
Suppress Printer Dialog (OC://WebPrint only)	Enable this option to bypass the system print dialog when a print request is made. This feature allows jobs to be sent directly to the default printer without user intervention and is supported only by the OC://WebPrint print solution.
Character Mode	Select this option to send one character at a time to a printer, allowing precise control of spacing and printing of attributes. By default, printing is performed in line mode, meaning text is sent one line at a time to the printer driver. In line mode, character spacing is determined by the printer driver and the selected font, so the right and bottom edges of the printed output are determined by this spacing rather than by margin settings. Attributes and printing to fixed metrics are not supported in line mode. **Note:** Character mode is not supported by the JavaScript print solution.
Raw Mode (3287 only)	Select this option to bypass the graphical print API, allowing printer-specific codes to be passed in the data stream and sent directly to the printer. This mode is required to support the SCS TRN (transparent) command. **Notes:** When raw mode is set, other mode settings and metric controls are ignored. Raw mode is supported by only the OC://WebPrint print solution and is used only in 3287 printing.
Printer Initialization String (in hex)	Type a string of hexadecimal bytes to send to the printer at the start of each print job. Spaces are ignored.
Printer Termination String (in hex)	Type a string of hexadecimal bytes to send to the printer at the end of each print job. Spaces are ignored.

Field	Procedure
Margin	Select **Pixels** or typographic **Points** as the unit of measurement for margin settings, which apply to both screen print and 3287 printing. In addition to the potential cosmetic use of this feature, print margin settings can be used to help with form alignment and to prevent data loss near paper edges. If there is no print margin, the print output for certain printers can be truncated near the edge of the paper. Appropriate print margins can be set to remedy the problem. A pixel is a logical unit of measure, specific to the print solution, while a typographic point is a physical unit of measure, normally equal to 1/72 inch. In some cases, it is appropriate to set the margins to 0. When working with the **Windows Generic/Text Only** printer driver, nonzero margins yield unpredictable results. Setting zero margins also allows JDK 1.1 Print to print uniformly, provided the **Typographic Point Size** is set to 72 both horizontally and vertically.
Left	Enter number of units to indent from left of page. Default is 20 pixels.
Right	Enter number of units to indent from right of page. Default is 20 pixels.
Top	Enter number of units from top of page to start printing.
Bottom	Enter the minimum number of units from bottom of page to leave blank.
Typographic Point Size	A typographic point is normally defined as 1/72 inch, but OC://WebConnect Pro allows you to modify this definition. This feature allows fine-grained scaling of print output, as might be required for fitting the output to a preprinted form.
Points Per Inch (horizontal)	Enter a number of horizontal points per inch to define a typographic point.
Points Per Inch (vertical)	Enter the number of vertical points per inch to define a typographic point.

☞

Troubleshooting

If the print method chosen is not supported by the browser or has not been installed or enabled on the browser platform, error messages might occur.

For more information about OC://WebConnect Pro printing solutions, see *Chapter 17: OC://WebConnect Pro Print Solutions.*

Scripting Settings

Field	Procedure
Startup	
Script	Type the name of the TCL script that automatically runs after a 3270 emulation session connects.
Arguments	Specify input arguments for the specified Startup TCL, for example, a user ID and password the script uses to log on to a host application. Separate arguments with a space. When using the GUI Configurator, specify the arguments in the Startup script field.
Runtime	
Script	Type the name of the script file that indicates run time for a 3270 session. Press **Ctrl+R** to start the script.
Arguments	Specify input arguments for the specified Startup TCL script, for example, a user ID and password the script uses to log on to a host application. Separate arguments with a space. When using the GUI Configurator, specify the arguments in the Startup script field.

☞

More Information

For more information, see *Chapter 13: TCL Scripting*.

Chapter 7: Configuring 5250 Emulation Sessions

Overview

OC://WebConnect Pro includes a feature-rich, 5250 emulation client with centralized configuration and administration on the server.

Session configuration is provided via centralized configuration and administration tools that can be accessed remotely through a browser. OC://WebConnect Pro provides two methods to configure OC://WebConnect Pro emulation sessions:

- The HTML onfiguration is a series of HTML pages that access the OC://WebConnect Pro server via a CGIbin interface to create, modify, and delete emulation session configurations via a browser. The HTML Configuration does not require a Java-enabled browser.

- The graphical **GUI Configurator** which is a Java applet downloaded to the browser platform and executed via a Java-enabled (JDK 1.1) browser.

Both configuration tools provide full-featured, remote session configuration to create, delete, and modify emulation sessions. An OC://WebConnect Pro server administrator can control important session configuration and management features like host access, security, session negotiation rules, and emulation interface configuration. If desired, the end user can be allowed to configure the keyboard, color, and attribute mapping.

Configuring 5250 Sessions Using HTML

The OC://WebConnect Pro HTML configuration is a series of HTML pages that retrieve the current server and session information from the OC://WebConnect Pro server through an administrative connection. An administrator can modify server settings and create, modify, or delete emulation session settings. The OC://WebConnect Pro server must be active to use the HTML configuration utility. See *Chapter 2: Starting OC://WebConnect Pro*.

Accessing the 5250 HTML Session Configuration Page

1. Connect to the OC://WebConnect Pro HTTP Web server: In the URL of a browser, type the following:

   - The host name where the OC://WebConnect Pro HTTP Web server is running
   - The TCP port number

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

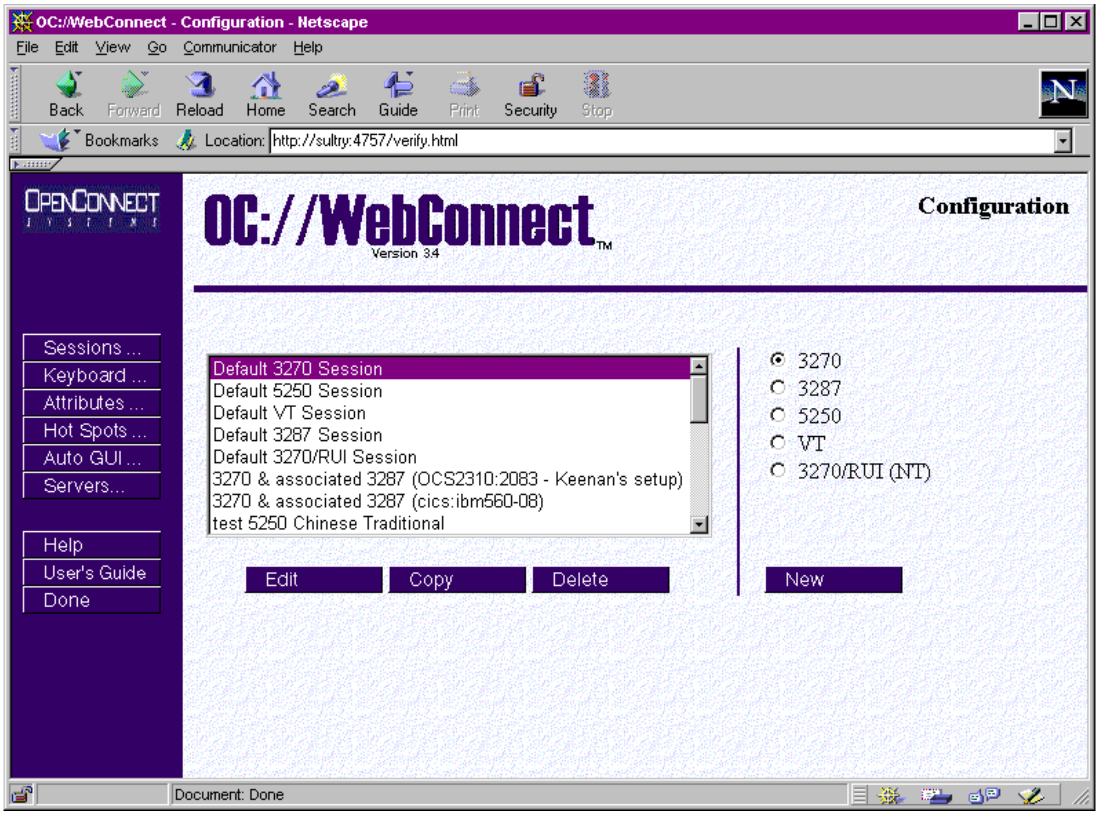
2. Press **Enter**. The **Start Sessions** page is displayed.

3. Click **Configuration** on the left of the **Start Sessions** page. A prompt appears for the **Administrator Password.**

4. Type the password in the box under **Enter Administrator Password** and click **OK**.

   ☞ **Note:** The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

   When the correct administrator password is entered, the main **Configuration** HTML page is displayed.



OC://WebConnect - Configuration - Netscape

Location: http://sultry:4757/verify.html

Default 3270 Session
Default 5250 Session
Default VT Session
Default 3287 Session
Default 3270/RUI Session
3270 & associated 3287 (OCS2310:2083 - Keenan's setup)
3270 & associated 3287 (cics:ibm560-08)
test 5250 Chinese Traditional

● 3270
○ 3287
○ 5250
○ VT
○ 3270/RUI (NT)

Document: Done

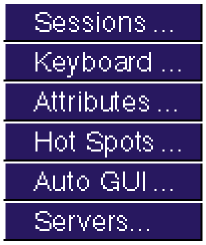
The main **Configuration** page has three sections:

- At the top is the **header** section, which shows the OC://WebConnect Pro version and the name of the HTML page displayed, **Configuration** in this example.

- On the left are **navigation buttons** used to access other OC://WebConnect Pro HTML pages for context-sensitive **Help**, the online **User's Guide**, and configuration pages for mapping other OC://WebConnect Pro features. The **Done** button exits this page.

- To the middle and right is the **session configuration** section used to create, edit, or delete session configurations.

Navigation Buttons



Sessions– Configure an individual session configuration. This page is displayed first.

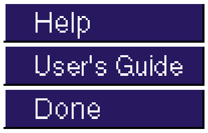
Keyboard – Create, modify, or delete a keyboard map.

Attributes – Create, modify, or delete an attribute and color map.

Hot Spots – Create, modify, or delete a hot spot map.

Auto GUI– Create, modify, or delete an auto GUI map.

Servers – Modify server settings.



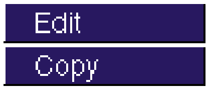
Access context-sensitive help.

Access online user guide.

Exit session configuration.

Session Configuration Buttons

A list of existing session configurations is displayed. To edit, copy, or delete an existing session, select a session and click the appropriate button.



Edit an existing session configuration.

Create a new session configuration from an existing session configuration.

Delete an existing session configuration.

A group of radio buttons indicates the supported emulation types. To create a new session configuration, choose an emulation type, and then click **New**.

Create a new session configuration.

Configuring a New 5250 Emulation Session Using HTML

1. Click the **5250** radio button.
2. Click **New**. A new session configuration page appears with the *default* session settings.
3. Type a unique session description and file name (without an extension).

   Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **5250**, **Display**, **Printing**, and **Scripting**. Modify the settings as needed.

   > **More Information**
   >
   > For more information about 5250 emulation features, see “5250 Emulation Session Features and Settings” in this chapter.

4. To save the new 5250 session configuration, click **Save** on the sidebar.

   -or-

   Click **Cancel** to abort creating the new session.

Editing an Existing 5250 Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Edit**. The first session configuration page appears with the chosen session description.
3. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **5250**, **Display**, **Printing**, and **Scripting**. Modify the settings as needed.

   > **More Information**
   >
   > For more information about 5250 emulation features, see “5250 Emulation Session Features and Settings” in this chapter.

4. To save the changes, click **Save** on the sidebar.

   -or-

   To cancel the changes made to the 5250 session configuration, click **Cancel** on the sidebar.

Copying an Existing 5250 Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Copy**. A new session configuration page appears with the same session settings.
3. Type a unique session description and file name.
4. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **5250**, **Display**, **Printing**, and **Scripting**. Modify the settings as needed.

> **More Information**
>
> For more information about 5250 emulation features, see “5250 Emulation Session Features and Settings” in this chapter.

5. To save the new 5250 emulation session configuration, click **Save** on the sidebar.

   -or-

   To abort creating a new 5250 session configuration, click **Cancel** on the sidebar.

Deleting an Existing 5250 Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Delete**. A new page appears requesting you to confirm the deletion.
3. Click **Delete** again to delete the selected session.

   -or-

   Click **Cancel** to stop the deletion.

> **Note:** Default session configurations cannot be deleted.

Configuring 5250 Sessions Using the GUI Configurator

After the OC://WebConnect Pro server is started (see *Chapter 2: Starting OC://WebConnect Pro*), you can access the GUI Configurator applet by selecting **GUI Config** on any OC://WebConnect *Pro* HTML page using a JDK 1.1 Java-enabled browser.

☞

More Information

You can restrict access to the GUI Configurator applet by removing the button from any OC://WebConnect Pro HTML page, or you can create custom HTML access to the GUI Configurator applet. See *Chapter 12: Customizing OC://WebConnect Pro*.

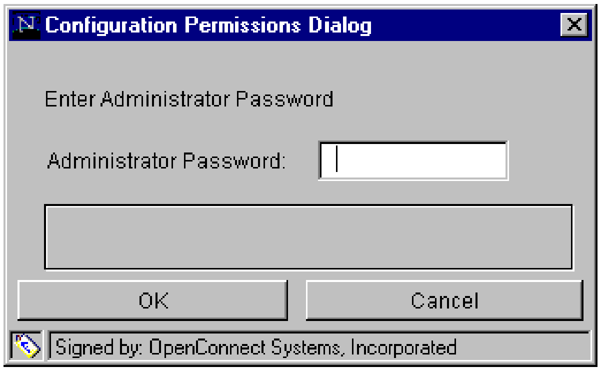
Accessing the GUI Configurator for 3287 Session Configuration

1. Start the OC://WebConnect Pro server. (See *Chapter 2: Starting OC://WebConnect Pro*.)

2. From any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser, click **GUI Config** on the sidebar. The browser downloads and starts the GUI Configurator applet.

   You might see one or more Java permissions windows. Click **Grant** in each window to authorize the applet to run.

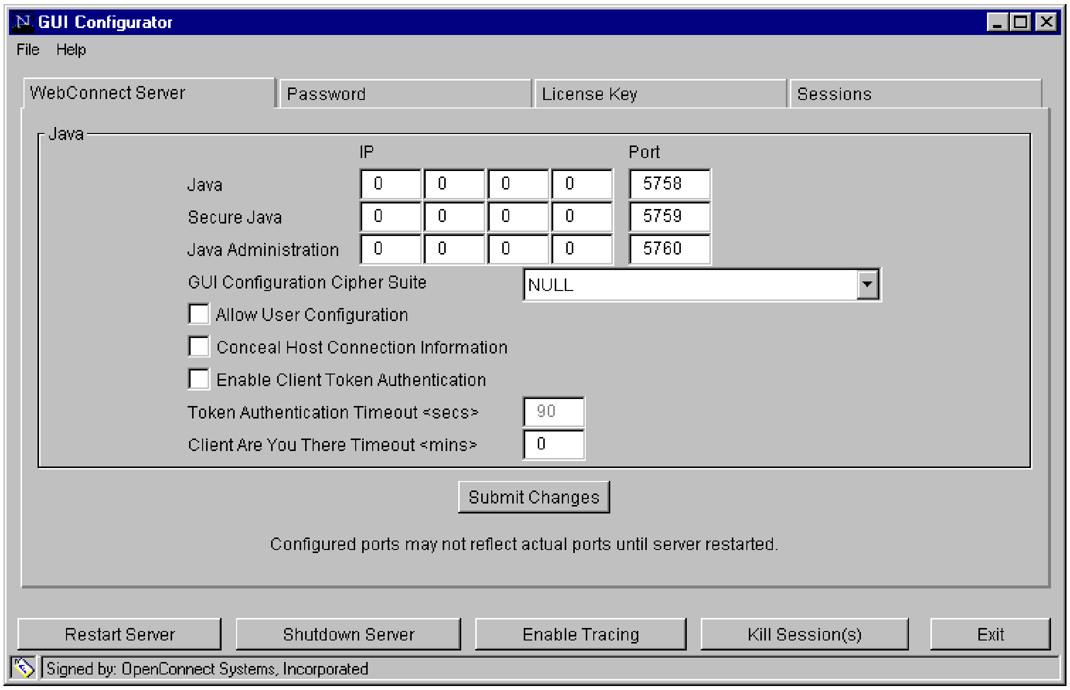
   After the applet starts, the **Configuration Permissions Dialog** window displays asking for the administrator password.


Configuration Permissions Dialog
Enter Administrator Password
Administrator Password:
OK
Cancel
Signed by: OpenConnect Systems, Incorporated

3. Type the password in the **Administrator Password** field and click **OK**.

Note: The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

When the correct administrator password is entered, the OC://WebConnect Pro **GUI Configurator** window, shown below, opens:



Java

	IP				Port
Java	0	0	0	0	5758
Secure Java	0	0	0	0	5759
Java Administration	0	0	0	0	5760

GUI Configuration Cipher Suite: NULL

□ Allow User Configuration

□ Conceal Host Connection Information

□ Enable Client Token Authentication

Token Authentication Timeout <secs> 90

Client Are You There Timeout <mins> 0

Configured ports may not reflect actual ports until server restarted.

Signed by: OpenConnect Systems, Incorporated

The window has four tabs at the top. The tab currently selected is OC://WebConnect Pro **Server**. The tab to work with in this section is **Sessions**.

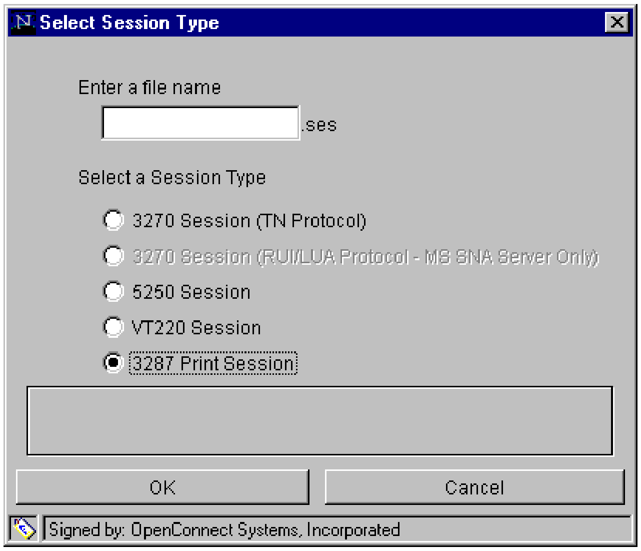
More Information

For more information on the OC://WebConnect **Server**, **Password**, and **License Key** tabs, see *Chapter 5: Server Configuration and Administration*.

Configuring a New 5250 Emulation Session

1. Click the **Sessions** tab on the OC://WebConnect Pro **GUI Configurator** window. A list of defined sessions displays.

2. Click **Create**. The **Select Session Type** window displays.



Enter a file name

[ ] .ses

Select a Session Type

○ 3270 Session (TN Protocol)
○ 3270 Session (RUI/LUA Protocol - MS SNA Server Only)
○ 5250 Session
○ VT220 Session
● 3287 Print Session

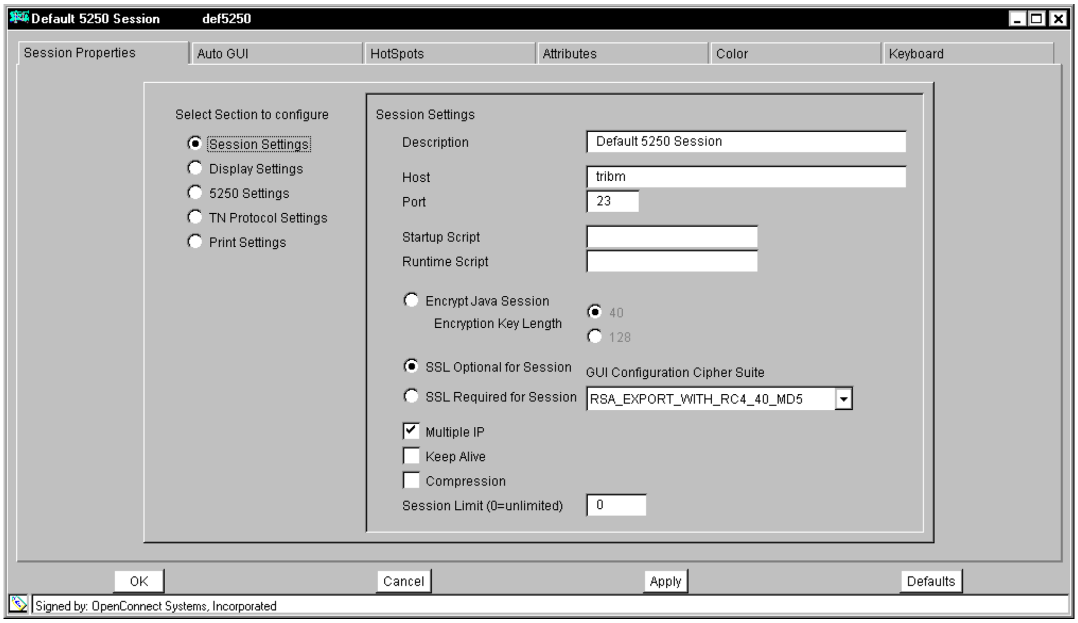
Signed by: OpenConnect Systems, Incorporated

3. Type a unique file name (without an extension) for the new session.

Notes

- When choosing a file name for a session configuration, consider that files are listed on the **Sessions** window in alphabetical order.
- To restore the form to default display values, click **Defaults**.

4. Select **5250 Session** and click **OK**. The **GUI Configurator** displays the **Session Properties** window for the selected emulator type. The configuration options are explained in “5250 Emulation Session Features and Settings” in this chapter.



Select Section to configure

● Session Settings
○ Display Settings
○ 5250 Settings
○ TN Protocol Settings
○ Print Settings

Session Settings

Description: Default 5250 Session

Host: tribm

Port: 23

Startup Script:

Runtime Script:

○ Encrypt Java Session

Encryption Key Length: ● 40 ○ 128

● SSL Optional for Session

○ SSL Required for Session

GUI Configuration Cipher Suite: RSA_EXPORT_WITH_RC4_40_MD5

☑ Multiple IP

□ Keep Alive

□ Compression

Session Limit (0=unlimited): 0

5. Modify **Session Settings** options as needed on the **Session Properties** window.

6. Click each radio button and modify settings if necessary:

   - Session Settings
   - Display Settings
   - 5250 Settings
   - TN Protocol Settings
   - Print Settings

7. Now, step through the other tabs—**Auto GUI**, **HotSpots**, **Attributes**, **Color**, and **Keyboard**—modifying settings as needed.

Notes

For more information about 5250 emulation features, see “5250 Emulation Session Features and Settings” in this chapter.

The tabs displayed depend on the mode the configuration applet is in and the emulation type of the session selected. For example, if the applet is in user mode, the **Sessions Properties** tab does not display.

8. Click **OK** to save the 5250 emulation session configuration.

   -or-

   Click **Cancel** to prevent creating the session configuration.

Editing a 5250 Session Configuration

1. Click the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to edit and click **Properties**. The **GUI Configurator** displays the **Session Properties** window for the selected emulation type.
3. Modify **Session Settings** options as needed on the **Session Properties** window.
4. Click each radio button and modify settings as needed:
   - **Session Settings**
   - **Display Settings**
   - **5250 Settings**
   - **TN Protocol Settings**
   - **Print Settings**
5. Now, step through the other tabs—**Auto GUI**, **HotSpots**, **Attributes**, **Color**, and **Keyboard**—modifying settings as needed.

☞

More Information

For more information about 5250 emulation features, see “5250 Emulation Session Features and Settings” in this chapter.

6. Click **OK** to save the 5250 emulation session configuration.

   -or-

   Click **Cancel** to prevent saving the changes.

Deleting a 5250 Emulation Session Configuration

1. Choose the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to delete and click **Delete**. A window is displayed requesting confirmation of the delete.
3. Click **OK** to confirm the deletion. The session file is deleted.

☞ **Note:** Default session files cannot be deleted.

5250 Emulation Session Features and Settings

Description

Field	Procedure
Description	Type a brief description for the session configuration. This description appears on windows used to select a session to start, modify, or delete.
Save as	Type a unique file name, without an extension, in which to store the emulation session settings.

5250 Network Settings

Field	Procedure
Connect to host	Enter the host name of the destination system. This can be the TCP/IP host name of the AS/400 system or of a gateway that provides TCP/IP services to the AS/400 system.
Port	Enter the TCP/IP port number of the gateway or TN server uses for emulation connections. The default Telnet port number is **23**.
Enable TCP/IP Keep Alive	Enable this option for OC://WebConnect Pro to utilize the Keep Alive feature of the underlying TCP/IP stack to monitor and clean up after unexpected session outages, such as PC client power losses or cable faults. Keep Alive monitors the connection from the browser client to the OC://WebConnect Pro server, as well as the connection from the OC://WebConnect Pro server to the Telnet server.
Try Multiple IP addresses	Enable this option if the host name being used for host connectivity refers to multiple DNS addresses. Multiple DNS addresses provide the OC://WebConnect Pro server a choice of gateways or TN servers when a server is busy or the session type is not available. **Note:** If this option is not enabled, only one connection attempt—to the first IP address returned—is made. OC://WebConnect Pro evaluates the DNS addresses serially to make a host connection, depending on the TN Server or gateway used. • If using an OC://WebConnect Pro SNA Access Server Gateway, evaluation is based on the availability of the specified model and LU type, a specific LU name, a specific LU number, and/or access to a specific SAC LU Pool. • If using a general TN server, evaluation is based on the model and/or LU type.

Field	Procedure
	Example: Host XY is configured for two IP addresses (gateway X and gateway Y). OC://WebConnect Pro wants a 3279 LU, and all 3279 LUs on gateway X are in use. OC://WebConnect Pro automatically attempts to connect to a 3279 LU on gateway Y.
Enable data compression	Enable this option to compress data flowing between the OC://WebConnect Pro server and the Java client. **Note:** The tradeoff for decreased network traffic is time spent compressing and decompressing data.

Security Settings

Field	Procedure
Diffie-Hellman/RC4 encryption	Enable this option to encrypt session data between the OC://WebConnect Pro server and Java client session. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both.
Key Length	Select **40 bits** or **128 bits**. 128-bit encryption is available only in the US. If 128-bit encryption is selected for a non-US version, the session defaults to 40-bit encryption. The encryption method for a specific emulation can be seen by selecting **Help**>**Help Desk**. **Note:** Key length in Ultra Lite session is always **40 bits**.
SSL	Enable SSL (Secure Socket Layer) to use an SSL cipher suite for authentication and/or encryption of data between the OC://WebConnect Pro server and the Java client session. This option requires that the OC://WebConnect Pro server Secure Java Port is configured and active. See *Chapter 5:* Server *Configuration and Administration* for more information about the Secure Java Port. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both. Select **Optional** to allow emulation client users to choose SSL or not. Select **Required** to force the use of SSL session configuration.
SSL Cipher Suite	Select an SSL Cipher Suite based on the level of security desired.
Limit number of sessions per applet	Enable this option to restrict the number of new sessions that can be started from an emulation session already connected. Each Java emulation client has a **File**>**New** menu item, which allows a new emulation session to be spawned from the existing connection. By default, an emulation client user can start as many sessions as the OC://WebConnect Pro license key allows.
sessions per applet	Specify the number of sessions that can be spawned from an emulation applet. Zero disables this option.

More Information

For more information about OC://WebConnect Pro security features, see *Chapter 15: Security Overview*.

Telnet Settings

Field	Procedure
Terminal Type Demotion	Click the check box to allow OC://WebConnect Pro to sequentially negotiate model types below the alternate screen size. The negotiation continues until a model is selected for the session. -or- Uncheck the check box to allow normal default and alternate screen sizes to be negotiated between OC://WebConnect Pro and the gateway.

5250 Settings

Field	Procedure
Device Type	Click the down arrow and choose the IBM device type to be emulated.
OC Server	Enable this option if an OpenConnect Systems gateway is to be used for host connections.
Auto Help	Enable this option to display error messages in the session's applet window.
AS400 V2R1 Support	Enable this option if the AS/400 host is using operating system version 2.0, release 1.0 or higher
PTS override	Enable this option to instruct OC://WebConnect Pro to send pass-through screen parameters to the 5250 host.
Remote Location Name	Enter a remote location name for the pass-through screen.
Mode Name	Enter a mode name for the pass-through screen.
Virtual Controller	Enter a virtual controller definition for the pass-through screen.
Virtual Display Device	Enter the name of the AS/400 virtual device.
Remote Network ID	Type a remote network identifier for the pass-through screen.
Local PU Name	Type a local PU name for the pass-through screen.
Local LU Name	Type a local LU name for the pass-through screen.

Display Settings

Field	Procedure
Language	Select the language to use for messages in the 5250 session emulation applet window.
Code Page	Enter the number of the code page for the target host application. Valid values are from 37 to 61712.
Transform Type	Select the code page transform type from the list box. **Note:** If using the Single/Double Byte EBCDIC-to-Unicode option, the ability to switch the single-byte code pages using a default key is available.
Font Size	Enter the number for the default font point size to use for text displayed in the applet window. This font size dictates the initial client window size.
Keyboard Map	Enter the keyboard map (**.kbm)** file name for the session being edited. The default is **def5250.kbm**.
Attribute Map	Enter the **.atm** file name for the session being edited. The default is **def5250.atm**.
Hot Spots	Enter the **.hsp** file name for the session being edited. The default is **def5250.hsp**.
Enable Auto GUI for this session.	Select this option to allow the emulation client user to toggle on or off the Auto GUI display option. If this option is disabled, the user does not have the Auto GUI option.
Auto GUI	Enter the **.agu** file name for the session being edited. The default is **def5250.agu**.
Clickpad	Enable this option to initially show a clickpad in an applet window. The clickpad can be used to select function keys or other special keys not mapped to the local keyboard.

☞

More Information

For more information about mapping user interface and display options, see *Chapter 10: Display Options Configuration and Features*.

Printing Settings

Field	Procedure
Radio buttons:	Select one.
Disabled	Select this option to disable screen print for this 5250 session.
OC://Webprint	Select this option to use OC://Webprint (Windows platform only) for screen print. OC://Webprint must be installed on the browser platform to use this solution. This option is supported on JDK 1.0 and greater browsers. The OC://WebPrint print solution is available in all OC://WebConnect Pro applets and avoids some problems associated with JDK 1.1 printing by printing at the resolution of the underlying print driver. OC://WebPrint prints to any paper size reported by the printer driver and honors all session settings and formatting controls from the data stream, generating uniformly spaced print output. In addition, OC://WebPrint supports two features not supported by the other print solutions: • A raw mode of operation that allows printer-specific codes to be passed in the data stream. • A suppress-printer-dialog option to allow jobs to be sent directly to the default printer without user intervention.
JavaScript	Select this option to use JavaScript, which is supported in some JDK 1.0 and greater browsers. The JavaScript print solution is supported by all OC://WebConnect Pro emulation applets. JavaScript functions are downloaded to the PC as part of the HTML page that loads the emulation applet. Therefore, if you write an HTML page to load the applet, the page must include JavaScript print functions to prevent breaking the JavaScript print solution. When printing with the JavaScript print solution, the JavaScript opens a separate browser window, writes the print output to that window, and then sends the browser contents to the system printer as if the user selected **File**>**Print** from the browser menu. JavaScript printing is convenient and provides a good print solution for applications not requiring control of the output format. Because the print output is rendered through the browser, the browser is in charge of formatting, and virtually all session settings and data stream commands related to formatting are ignored.
JDK 1.1 Print	Select this option for screen print using JDK 1.1 print methods embedded in JDK 1.1-based browsers. The JDK 1.1 print solution is the native print implementation provided by all browsers utilizing JDK 1.1 or later, making it available when using an Enhanced or Power User applet. The browser's JVM (Java

Field	Procedure
	Virtual Machine) implementing JDK 1.1 printing prints at a fixed resolution, typically 72 or 96 pixels per inch, which is usually less than the resolution of the attached printer. This mismatch causes incompatibilities with the **Windows Generic/Text Only** driver and can cause nonuniform character spacing when attempting to print at specified line and/or character densities. Printing with the **Auto Fit** feature enabled prevents the latter problem. **Note:** Screen printing always prints in **Auto Fit** mode. Early versions of JDK 1.1 implemented in most browsers contain bugs that affect the ability of OC://WebConnect Pro to properly determine the page size. In these older browsers, the page size is assumed to be 8.5-by-11-inch paper in portrait mode. As of JDK 1.1.4, most of these bugs have been fixed, allowing support of landscape mode and other paper sizes.
Suppress Printer Dialog (OC://WebPrint only)	Enable this option to bypass the system print dialog when a print request is made. This feature allows jobs to be sent directly to the default printer without user intervention and is supported only by the OC://WebPrint print solution.
Character Mode	Select this option to send one character at a time to a printer, allowing precise control of spacing and printing of attributes. By default, printing is performed in line mode, meaning text is sent one line at a time to the printer driver. In line mode, character spacing is determined by the printer driver and the selected font, so the right and bottom edges of the printed output are determined by this spacing rather than by margin settings. Attributes and printing to fixed metrics are not supported in line mode. **Note:** Character mode is not supported by the JavaScript print solution.
Margin	Select **Pixels** or typographic **Points** as the unit of measurement for margin settings, which apply to both screen print and 3287 printing. In addition to the potential cosmetic use of this feature, print margin settings can be used to help with form alignment and to prevent data loss near paper edges. If there is no print margin, the print output for certain printers can be truncated near the edge of the paper. Appropriate print margins can be set to remedy the problem. A pixel is a logical unit of measure, specific to the print solution, while a typographic point is a physical unit of measure, normally equal to 1/72 inch. In some cases, it is appropriate to set the margins to 0. When working with the **Windows Generic/Text Only** printer driver, nonzero margins yield unpredictable results. Setting zero margins also allows JDK 1.1 Print to print uniformly, provided the **Typographic Point Size** is set to 72 both horizontally and vertically.
Left	Enter number of units to indent from left of page. Default is 20 pixels.

Field	Procedure
Right	Enter number of units to indent from right of page. Default is 20 pixels.
Top	Enter number of units from top of page to start printing.
Bottom	Enter the minimum number of units from bottom of page to leave blank.
Typographic Point Size	A typographic point is normally defined as 1/72 inch, but OC://WebConnect Pro allows you to modify this definition. This feature allows fine-grained scaling of print output, as might be required for fitting the output to a preprinted form.
Points Per Inch (horizontal)	Enter a number of horizontal points per inch to define a typographic point.
Points Per Inch (vertical)	Enter the number of vertical points per inch to define a typographic point.

☞

Troubleshooting

If the print method chosen is not supported by the browser or has not been installed or enabled on the browser platform, error messages might occur.

For more information about OC://WebConnect Pro printing solutions, see *Chapter 17: OC://WebConnect Pro Print Solutions*.

Scripting Settings

Field	Procedure
Startup	
Script	Type the name of the TCL script that automatically runs after a 5250 emulation session connects.
Arguments	Specify input arguments for the specified Startup TCL, for example, a user ID and password the script uses to log on to a host application. Separate arguments with a space. When using the GUI Configurator, specify the arguments in the Startup script field.
Runtime	
Script	Type the name of the script file that indicates run time for a 5250 session. Press **Ctrl+R** to start the script.
Arguments	Specify input arguments for the specified Startup TCL script, for example, a user ID and password the script uses to log on to a host application. Separate arguments with a space. When using the GUI Configurator, specify the arguments in the Startup script field.

☞

More Information

For more information, see *Chapter 13: TCL Scripting Extensions*.

Chapter 8: Configuring 3287 Print Emulation Sessions

Overview

OC://WebConnect Pro combines a feature-rich, 3287 print emulation client with centralized configuration and administration on the server.

Session configuration is provided via centralized configuration and administration tools that can be accessed remotely through a browser. OC://WebConnect Pro provides two methods to configure OC://WebConnect Pro emulation sessions:

- The HTML configuration is a series of HTML pages that access the OC://WebConnect Pro server via a common gateway interface (CGI) interface to create, modify, and delete emulation session configurations via a browser. The HTML Configuration does not require a Java-enabled browser.
- The graphical **GUI Configurator** which is a Java applet downloaded to the browser platform and executed via a Java-enabled (JDK 1.1) browser.

Both configuration tools provide full-featured, remote session configuration to create, delete, and modify emulation sessions. An OC://WebConnect Pro server administrator can control important session configuration and management features like host access, security, session negotiation rules, and emulation interface configuration. If desired, the end user can be allowed to configure the keyboard, color, and attribute mapping.

Configuring 3287 Sessions Using HTML

The OC://WebConnect Pro HTML configuration is a series of HTML pages that retrieve the current server and session information from the OC://WebConnect Pro server through an administrative connection. An administrator can modify server settings and create, modify, or delete emulation session settings. The OC://WebConnect Pro server must be active to use the HTML configuration utility. See *Chapter 2: Starting OC://WebConnect Pro*.

Accessing the 3287 HTML Session Configuration Page

1. Connect to the OC://WebConnect Pro HTTP Web server: In the URL of a browser, type the following:

   - The host name where the OC://WebConnect Pro HTTP Web server is running
   - The TCP port number

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

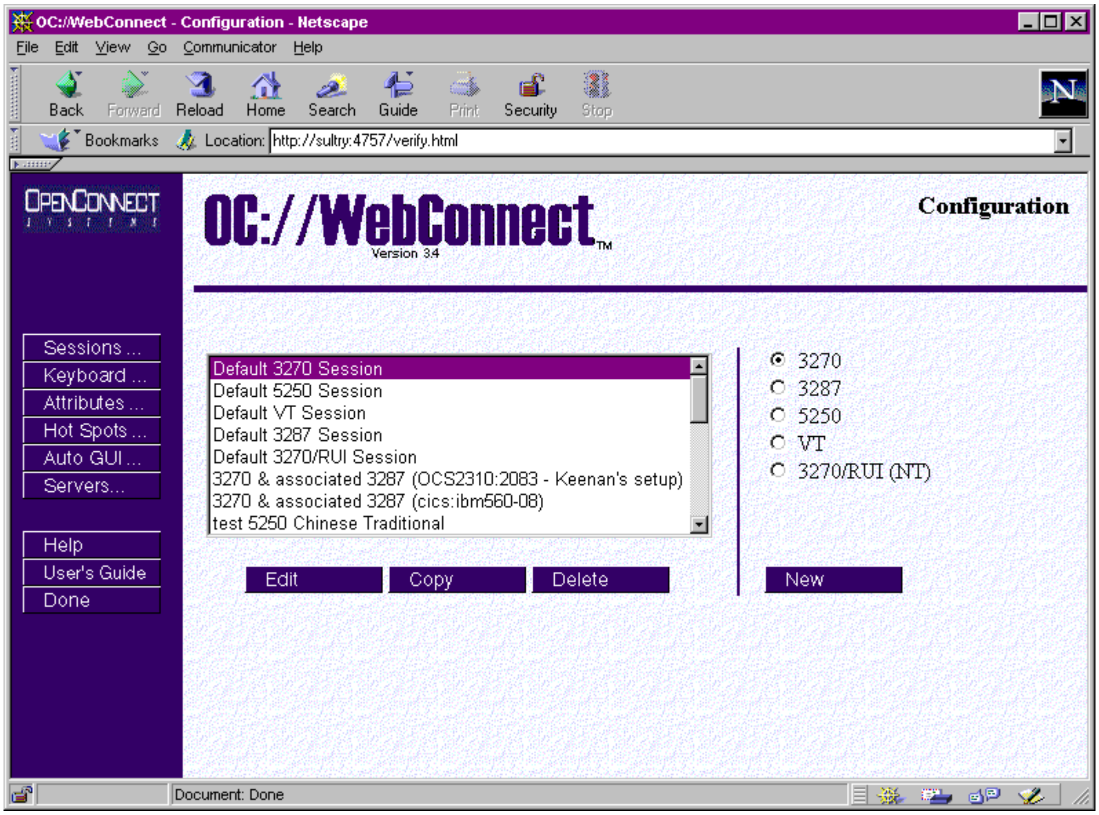
2. Press **Enter**. The **Start Sessions** page is displayed.

3. Click **Configuration** on the left of the **Start Sessions** page. A prompt appears for the **Administrator Password.**

4. Type the password in the box under **Enter Administrator Password** and click **OK**.

   ☞ **Note:** The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

   When the correct administrator password is entered, the main **Configuration** HTML page is displayed.


OC://WebConnect - Configuration - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://sultry:4757/verify.html
OPENCONNECT SYSTEMS
OC://WebConnect
Version 3.4
Configuration
Sessions ...
Keyboard ...
Attributes ...
Hot Spots ...
Auto GUI ...
Servers...
Help
User's Guide
Done
Edit
Copy
Delete
New
Document: Done

Default 3270 Session
Default 5250 Session
Default VT Session
Default 3287 Session
Default 3270/RUI Session
3270 & associated 3287 (OCS2310:2083 - Keenan's setup)
3270 & associated 3287 (cics:ibm560-08)
test 5250 Chinese Traditional

● 3270
○ 3287
○ 5250
○ VT
○ 3270/RUI (NT)

The main **Configuration** page has three sections:

- At the top is the **header** section, which shows the OC://WebConnect Pro version and the name of the HTML page displayed, **Configuration** in this example.
- On the left are **navigation buttons** used to access other OC://WebConnect Pro HTML pages for context-sensitive **Help**, the online **User's Guide**, and configuration pages for mapping other OC://WebConnect Pro features. The **Done** button exits this page.
- To the middle and right is the **session configuration** section used to create, edit, or delete session configurations.

Navigation Buttons

Sessions – Configure an individual session configuration. This page is displayed first.

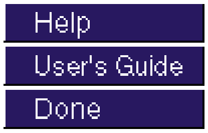
Keyboard – Create, modify, or delete a keyboard map.

Attributes – Create, modify, or delete an attribute and color map.

Hot Spots – Create, modify, or delete a hot spot map.

Auto GUI – Create, modify, or delete an auto GUI map.

Servers – Modify server settings.



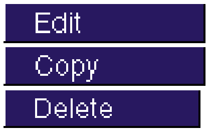
Access context-sensitive help.

Access the online user guide.

Exit session configuration.

Session Configuration Buttons

A list of existing session configurations is displayed. To edit, copy, or delete an existing session, select a session and click a button.



Edit an existing session configuration.

Create a new session configuration from an existing session configuration.

Delete an existing session configuration.

A group of radio buttons indicates the supported emulation types. To create a new session configuration, choose an emulation type, and then click **New**.

Create a new session configuration.

Configuring a New 3287 Print Session Using HTML

1. Click the **3287** radio button.
2. Click **New**. A new session configuration page appears with the *default* session settings.
3. Type a unique session description and file name (without an extension).

   Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **3287**, **Display**, and **Printing**. Modify the settings as needed.

> **More Information**
>
> For more information about 3287 emulation features, see "3287 Print Session Features and Settings" in this chapter.

4. To save the new 3287 session configuration, click **Save** on the sidebar.

   -or-

   Click **Cancel** to abort creating the new session.

Editing an Existing 3287 Print Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Edit**. The first session configuration page appears with the chosen session description.

   Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **3287**, **Display**, and **Printing**. Modify the settings as needed.

> **More Information**
>
> For more information about 3287 emulation features, see "3287 Print Session Features and Settings" in this chapter.

3. To save the changes, click **Save** on the sidebar.

   -or-

   To cancel the changes made to the 3287 session configuration, click **Cancel** on the sidebar.

Copying an Existing 3287 Print Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Copy**. A new session configuration page appears with the same session settings.
3. Type a unique session description and file name.

   Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **3287**, **Display**, and **Printing**. Modify the settings as needed.

☞

More Information

For more information about 3287 emulation features, see “3287 Print Session Features and Settings” in this chapter.

4. To save the new 3287 print session configuration, click **Save** on the sidebar.

   -or-

   To abort creating a new 3287 session configuration, click **Cancel** on the sidebar.

Deleting a 3287 Print Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Delete**. A new page appears requesting you to confirm the deletion.
3. Click **Delete** again to delete the selected session.

   -or-

   Click **Cancel** to stop the deletion.

☞

Note: Default session configurations cannot be deleted.

Configuring 3287 Sessions Using the GUI Configurator

After the OC://WebConnect Pro server is started (see *Chapter 2: Starting OC://WebConnect Pro*), you can access the GUI Configurator applet by selecting **GUI Config** on any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser.

More Information

You can restrict access to the GUI Configurator applet by removing the button from any OC://WebConnect Pro HTML page, or you can create custom HTML access to the GUI Configurator applet. See *Chapter 12: Customizing OC://WebConnect Pro*.

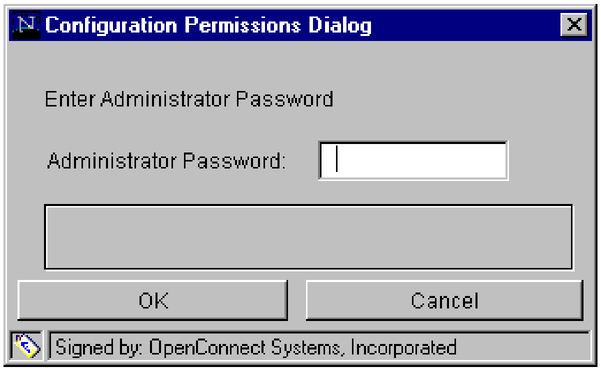
Accessing the GUI Configurator for 3287 Session Configuration

1. Start the OC://WebConnect Pro server. (See *Chapter 2: Starting OC://WebConnect Pro*.)

2. From any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser, click **GUI Config** on the sidebar. The browser downloads and starts the GUI Configurator applet.

   You might see one or more Java permissions windows. Click **Grant** in each window to authorize the applet to run.

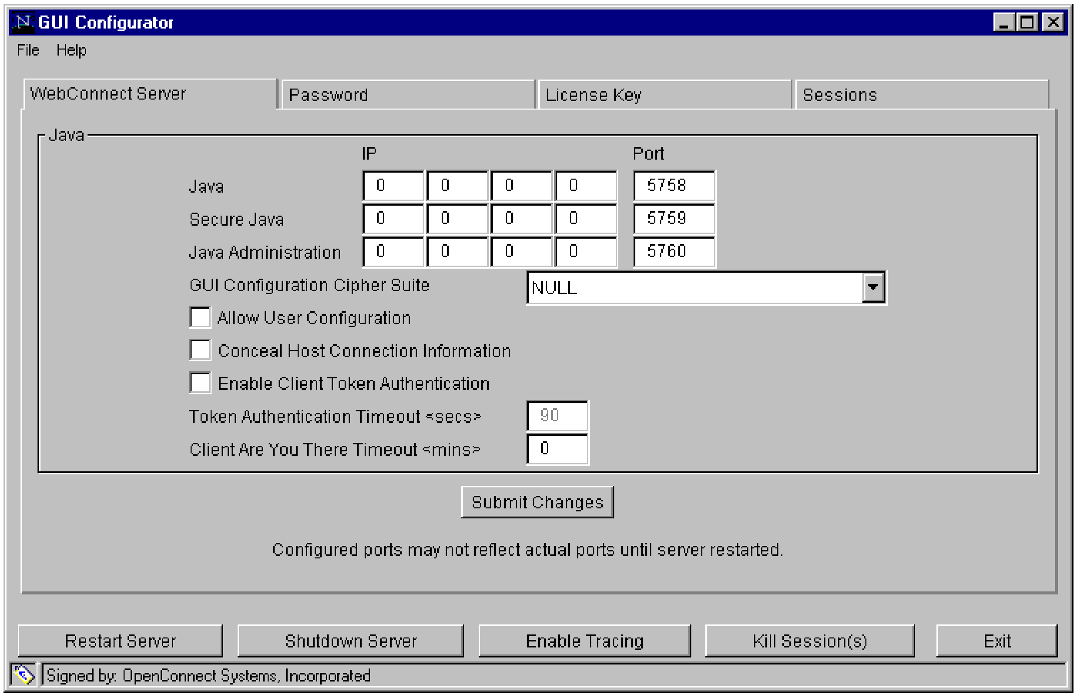
   After the applet starts, the **Configuration Permissions Dialog** window displays asking for the administrator password.


Configuration Permissions Dialog
Enter Administrator Password
Administrator Password:
OK
Cancel
Signed by: OpenConnect Systems, Incorporated

3. Type the password in the **Administrator Password** field and click **OK**.

Note: The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

When the correct administrator password is entered, the OC://WebConnect Pro **GUI Configurator** window, shown below, opens:



	IP				Port
Java	0	0	0	0	5758
Secure Java	0	0	0	0	5759
Java Administration	0	0	0	0	5760

GUI Configuration Cipher Suite NULL

□ Allow User Configuration

□ Conceal Host Connection Information

□ Enable Client Token Authentication

Token Authentication Timeout <secs> 90

Client Are You There Timeout <mins> 0

Configured ports may not reflect actual ports until server restarted.

Signed by: OpenConnect Systems, Incorporated

The window has four tabs at the top. The tab currently selected is **Server**. The tab to work with in this section is **Sessions**.

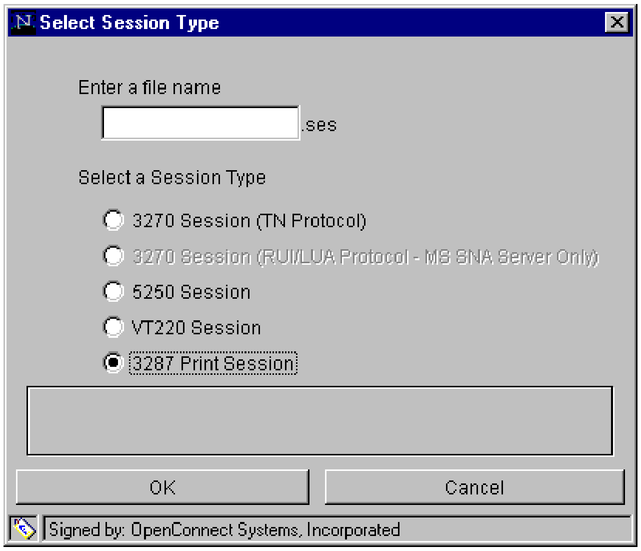
More Information

For more information on the OC://WebConnect Pro **Server**, **Password**, and **License Key** tabs, see *Chapter 5: Server Configuration and Administration*.

Configuring a New 3287 Print Emulation Session

1. Click the **Sessions** tab on the OC://WebConnect Pro **GUI Configurator** window. A list of defined sessions displays.

2. Click **Create**. The **Select Session Type** window displays.


Select Session Type
Enter a file name
.ses
Select a Session Type
○ 3270 Session (TN Protocol)
○ 3270 Session (RUI/LUA Protocol - MS SNA Server Only)
○ 5250 Session
○ VT220 Session
● 3287 Print Session
OK
Cancel
Signed by: OpenConnect Systems, Incorporated

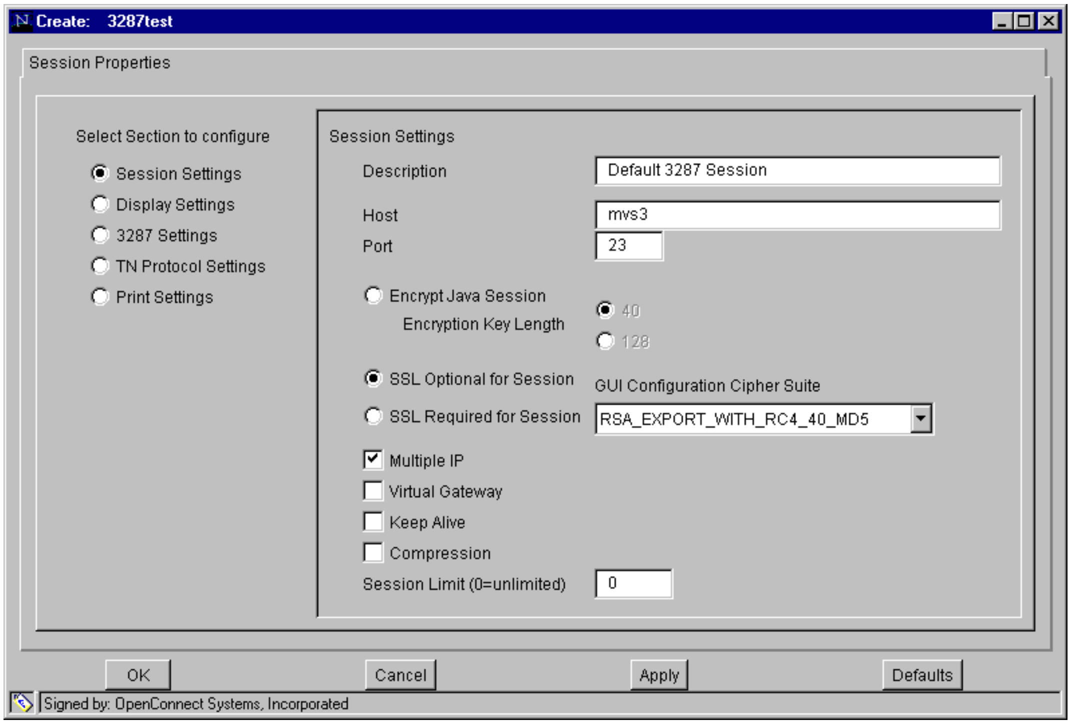
3. Type a unique file name (without an extension) for the new session.

☞

Notes

- When choosing a file name for a session configuration, consider that files are listed on the **Sessions** window in alphabetical order.
- To restore the form to default display values, click **Defaults**.

4. Select **3287 Print Session** and click **OK**. The **GUI Configurator** displays the **Session Properties** window for the selected emulator type. The configuration options are explained in "3287 Print Session Features and Settings" in this chapter.



Session Properties

Select Section to configure

- ● Session Settings
- ○ Display Settings
- ○ 3287 Settings
- ○ TN Protocol Settings
- ○ Print Settings

Session Settings

Description	Default 3287 Session
Host	mvs3
Port	23
○ Encrypt Java Session Encryption Key Length	● 40 ○ 128
● SSL Optional for Session	GUI Configuration Cipher Suite
○ SSL Required for Session	RSA_EXPORT_WITH_RC4_40_MD5
☑ Multiple IP	
□ Virtual Gateway	
□ Keep Alive	
□ Compression	
Session Limit (0=unlimited)	0

Signed by: OpenConnect Systems, Incorporated

5. Modify **Session Settings** options as needed on the **Session Properties** window.

6. Click each radio button and modify settings if necessary:

   - **Display Settings**
   - **3287 Settings**
   - **TN Protocol Settings**
   - **Print Settings**

More Information

For more information about 3287 print emulation features, see “3287 Print Session Features and Settings” in this chapter.

7. Click **OK** to save the 3287 print session configuration.

   -or-

   Click **Cancel** to prevent creating the session configuration.

Editing a 3287 Print Session Configuration

1. Click the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to edit and click **Properties**. The **GUI Configurator** displays the **Session Properties** window for the selected emulation type.
3. Modify **Session Settings** options as needed on the **Session Properties** window.
4. Click each radio button and modify settings as needed:
    - **Display Settings**
    - **3287 Settings**
    - **TN Protocol Settings**
    - **Print Settings**

> **More Information**
>
> For more information about 3287 print emulation features, see “3287 Print Session Features and Settings” in this chapter.

5. Click **OK** to save the 3287 print session configuration.

   -or-

   Click **Cancel** to prevent saving the changes.

Deleting a 3287 Print Session Configuration

1. Choose the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to delete and click **Delete**. A window is displayed requesting confirmation of the delete.
3. Click **OK** to confirm the deletion. The session file is deleted.

> **Note:** Default session files cannot be deleted.

3287 Print Session Features and Settings

Description

Field	Procedure
Description	Type a brief description for the session configuration. This description appears on windows used to select a session to start, modify, or delete.
Save as	Type a unique file name, without an extension, in which to store the emulation session settings.

Network Settings

Field	Procedure
Connect to host	Enter the host name of the destination system. This can be the TCP/IP host name of the destination system or of a gateway that provides TCP/IP services to the destination system.
Port	Enter the TCP/IP port number of the gateway or TN server used for emulation connections. The default Telnet port number is **23**.
Enable TCP/IP Keep Alive	Enable this option for OC://WebConnect Pro to utilize the Keep Alive feature of the underlying TCP/IP stack to monitor and clean up after unexpected session outages, such as PC client power losses or cable faults. Keep Alive monitors the connection from the browser client to the OC://WebConnect Pro server, as well as the connection from the OC://WebConnect Pro server to the TN3270 server.
Try Multiple IP addresses	Enable this option if the host name being used for host connectivity refers to multiple DNS addresses. Multiple DNS addresses provide the OC://WebConnect Pro server a choice of gateways or TN servers when a server is busy or the session type is not available. **Note:** If this option is not enabled, only one connection attempt—to the first IP address returned—is made. OC://WebConnect Pro evaluates the DNS addresses serially to make a host connection, depending on the TN Server or gateway used. • If using an OC://WebConnect SNA Access Server Gateway, evaluation is based on the availability of the specified model and LU type, a specific LU name, a specific LU number, and/or access to a specific SAC LU Pool. • If using a TN3270E server, evaluation is based on the model and LU type or a specific LU name.

Field	Procedure
	• If using a general TN server, evaluation is based on the model and/or LU type. Example: Host XY is configured for two IP addresses (gateway X and gateway Y). OC://WebConnect Pro wants a 3279 LU, and all 3279 LUs on gateway X are in use. OC://WebConnect Pro automatically attempts to connect to a 3279 LU on gateway Y.
Use virtual gateway	Enable this option to instruct OC://WebConnect Pro to access an OpenConnect Systems virtual gateway to the host gateway for this client location. This option requires an SNA Access Server Gateway.
Enable data compression	Enable this option to compress data flowing between the OC://WebConnect Pro server and the Java client. **Note:** The tradeoff for decreased network traffic is time spent compressing and decompressing data.

Security Settings

Field	Procedure
Diffie-Hellman/RC4 encryption	Enable this option to encrypt session data between the OC://WebConnect Pro server and Java client session. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both.
Key Length	Select **40 bits** or **128 bits**. 128-bit encryption is available only in the US. If 128-bit encryption is selected for a non-US version, the session defaults to 40-bit encryption. The encryption method for a specific emulation can be seen by selecting **Help**>**Help Desk**. **Note:** Key length in Ultra Lite session is always **40 bits**.
SSL	Enable SSL (Secure Socket Layer) to use an SSL cipher suite for authentication and/or encryption of data between the OC://WebConnect Pro server and the Java client session. This option requires that the OC://WebConnect Pro server Secure Java Port is configured and active. See *Chapter 5: Server Configuration and Administration* for more information about the Secure Java Port. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both. Select **Optional** to allow emulation client users to choose SSL or not. Select **Required** to force the use of SSL session configuration.
SSL Cipher Suite	Select an SSL Cipher Suite based on the level of security desired.

Field	Procedure
Limit number of sessions per applet	Enable this option to restrict the number of new sessions that can be started from an emulation session already connected. Each Java emulation client has a **File**>**New** menu item, which allows a new emulation session to be spawned from the existing connection. By default, an emulation client user can start as many sessions as the OC://WebConnect Pro license key allows.
sessions per applet	Specify the number of sessions that can be spawned from an emulation applet. Zero disables this option.

☞

More Information

For more information about OC://WebConnect Pro security features, see *Chapter 15: Security Overview*.

Telnet Settings

Field	Procedure
Enable TN3270E	Check this box if the gateway or host TN server supports the enhanced TN3270 protocol, TN3270E. Enabling TN3270E allows the use of the Associate 3287 Printer feature.
IP Pass Through	This parameter specifies whether IP pass through is enabled. • On – IP pass through is enabled and displays the negotiated IP address. • Off – IP pass through is not enabled. **Notes:** RTM support and IP pass through require an SNA Access Server Gateway version 3.8 or greater. Any other gateway must have IP pass through disabled. If the SNA Access Server Gateway has IP Health Check enabled, IP pass through is required, and RTM support is optional.
RTM Support	Click the check box to extend Response Time Monitoring (RTM) from the OC://WebConnect Pro server to the client. See notes above.

Field	Procedure
Telnet AYT -	Click the check box to instruct OC://WebConnect Pro to send “Are you there” messages to the host to maintain the connection between the OC://WebConnect Pro server and the gateway or Telnet server during periods of user or host inactivity. If this check box is not selected, messages are not sent to the host.
Idle Timeout minutes	Enter a value in whole minutes for OC://WebConnect Pro to wait for an AYT response from the remote host.
Device Names	Type one or more LU or Pool names of the OCS gateway, separated by a space.

3287 Settings

Field	Procedure
Default Format Values	The default values described below can be overridden by commands in the data stream. The data stream can also issue commands that revert the session to default settings, causing these values to again take effect.
Characters Per Line	This setting corresponds to the MPP (Maximum Presentation Position) parameter defined for LU1 printing passed in the SHF (Set Horizontal Format) command. It also defines the end-of-line position for LU3 printing when the WCC printout format bits are set to 00. See **Wrap Lines Exceeding Line Length** below.
Lines Per Page	This setting corresponds to the MPL (Maximum Presentation Line) parameter defined for LU1 printing passed in the SVF (Set Vertical Format). The setting has no meaning in LU3 printing. See **Break Pages Exceeding Page Length** below.
Point Font Size	This setting corresponds to the LD (Line Density) parameter defined for LU1 printing passed in the SLD (Set Line Density) command. It also defines the font size used for LU3 printing when the **Auto Fit** option is disabled. If character mode is not enabled, the current value of LD is used directly as the font size and the line spacing is the default line spacing of the font. If character mode is enabled, the line spacing is computed as the Vertical Points Per Inch/Point Font Size. The font size is then chosen to fit the vertical and horizontal spacing.
Characters Per Inch	This setting, also know as character pitch, corresponds to the PD (Print Density) parameter defined for LU1 printing passed in the SPD (Set Print Density) command. It also defines the print density used for LU3 printing when the **Auto Fit** option is disabled. If this parameter is set to 0 and no SPD command is received in the data stream, or if character mode is not enabled, then the print output is printed in the default character spacing of the active font.

Field	Procedure
Auto Fit	Select this option to format the print output to fit the paper size. **Notes:** If this option is not enabled, the print font size is effectively fixed such that 80-column documents fit a portrait page setting, and 132-column documents fit a landscape page setting. In this mode, 132-column documents can overflow a portrait page. Setting AutoFit causes the 3287 applet to select a font for the current page setting, ensuring that lines are not truncated. The JavaScript print method does not support the Auto Fit feature.
Wrap Lines Exceeding Line Length	Setting this option causes the **Characters Per Line** setting to be honored, resulting in the automatic insertion of a New Line operation if an attempt is made to write beyond the right margin (as defined in the SHF command—*not* the margins set in the **Printing** settings for the session). This option is normally enabled. Disabling the option can be useful for applications to operate in raw mode and pass escape sequences through to the printer without risking the automatic insertion of a New Line character into the escape sequence.
Break Pages Exceeding Page Length	Setting this option causes the **Lines Per Page** setting to be honored, resulting in the automatic insertion of a Form Feed operation if an attempt is made to write beyond the current bottom margin (as defined in the SVF command—*not* the margins set in the **Printing** settings for the session). This option is normally enabled. Disabling this option can be useful for applications to operate in raw mode and pass escape sequences through to the printer without risking the automatic insertion of a Form Feed character into the escape sequence.

Display Settings

Field	Procedure
Language	Select the language to use for messages in the 3287 session emulation applet window.
Code Page	Enter the number of the code page for the target host application. Values range from 37 to 61712.
Transform Type	Select the code page transform type from the list box. **Note:** If using the Single/Double Byte EBCDIC-to-Unicode option, the ability to switch the single-byte code pages using a default key is available.

Printing Settings

Field	Procedure
Radio buttons:	Select one.
OC://Webprint	Select this option to use OC://Webprint (Windows platform only) for screen print. OC://Webprint must be installed on the browser platform to use this solution. This option is supported on JDK 1.0 and greater browsers. The OC://WebPrint print solution is available in all OC://WebConnect Pro applets and avoids some problems associated with JDK 1.1 printing by printing at the resolution of the underlying printer driver. OC://WebPrint prints to any paper size reported by the printer driver and honors all session settings and formatting controls from the data stream, generating uniformly spaced print output. In addition, OC://WebPrint supports two features not supported by the other print solutions: • A raw mode of operation that allows printer-specific codes to be passed in the data stream. • A suppress-printer-dialog option to allow jobs to be sent directly to the default printer without user intervention.
JavaScript	Select this option to use JavaScript, which is supported in some JDK 1.0 and greater browsers. The JavaScript print solution is supported by all OC://WebConnect Pro emulation applets. JavaScript functions are downloaded to the PC as part of the HTML page that loads the emulation applet. Therefore, if you write an HTML page to load the applet, the page must include JavaScript print functions to prevent breaking the JavaScript print solution. When printing with the JavaScript print solution, the JavaScript opens a separate browser window, writes the print output to that window, and then sends the browser contents to the system printer as if the user selected **File**>**Print** from the browser menu. JavaScript printing is convenient and provides a good print solution for applications not requiring control of the output format. Because the print output is rendered through the browser, the browser is in charge of formatting, and virtually all session settings and data stream commands related to formatting are ignored.
JDK 1.1 Print	Select this option for screen print and 3287 printing using JDK 1.1 print methods embedded in JDK 1.1-based browsers. The JDK 1.1 print solution is the native print implementation provided by all browsers utilizing JDK 1.1 or later, making it available when using an Enhanced or Power User applet. The browser’s JVM (Java Virtual Machine) implementing JDK 1.1 printing prints at a fixed resolution, typically 72 or 96 pixels per inch, which is usually less than

Field	Procedure
	the resolution of the attached printer. This mismatch causes incompatibilities with the **Windows Generic/Text Only** driver and can cause nonuniform character spacing when attempting to print at specified line and/or character densities. Printing with the **Auto Fit** feature enabled prevents the latter problem. **Note:** Screen printing always prints in **Auto Fit** mode. Early versions of JDK 1.1 implemented in most browsers contain bugs that affect the ability of OC://WebConnect Pro to properly determine the page size. In these older browsers, the page size is assumed to be 8.5-by-11-inch paper in portrait mode. As of JDK 1.1.4, most of these bugs have been fixed, allowing support of landscape mode and other paper sizes.
Suppress Printer Dialog (OC://WebPrint only)	Enable this option to bypass the system print dialog when a print request is made. This feature allows jobs to be sent directly to the default printer without user intervention and is supported only by the OC://WebPrint print solution.
Character Mode	Select this option to send one character at a time to a printer, allowing precise control of spacing and printing of attributes. By default, printing is performed in line mode, meaning text is sent one line at a time to the printer driver. In line mode, character spacing is determined by the printer driver and the selected font, so the right and bottom edges of the printed output are determined by this spacing rather than by margin settings. Attributes and printing to fixed metrics are not supported in line mode. **Note:** Character mode is not supported by the JavaScript print solution.
Raw Mode (3287 only)	Select this option to bypass the graphical print API, allowing printer-specific codes to be passed in the data stream and sent directly to the printer. This mode is required to support the SCS TRN (transparent) command. **Notes:** When raw mode is set, other mode settings and metric controls are ignored. Raw mode is supported by only the OC://WebPrint print solution and is used only in 3287 printing.
Printer Initialization String (in hex)	Type a string of hexadecimal bytes to send to the printer at the start of each print job. Spaces are ignored.
Printer Termination String (in hex)	Type a string of hexadecimal bytes to send to the printer at the end of each print job. Spaces are ignored.

Field	Procedure
Margin	Select **Pixels** or typographic **Points** as the unit of measurement for margin settings, which apply to both screen print and 3287 printing. In addition to the potential cosmetic use of this feature, print margin settings can be used to help with form alignment and to prevent data loss near paper edges. If there is no print margin, the print output for certain printers can be truncated near the edge of the paper. Appropriate print margins can be set to remedy the problem. A pixel is a logical unit of measure, specific to the print solution, while a typographic point is a physical unit of measure, normally equal to 1/72 inch. In some cases, it is appropriate to set the margins to 0. When working with the **Windows Generic/Text Only** printer driver, nonzero margins yield unpredictable results. Setting zero margins also allows JDK 1.1 Print to print uniformly, provided the **Typographic Point Size** is set to 72 both horizontally and vertically.
Left	Enter number of units to indent from left of page. Default is 20 pixels.
Right	Enter number of units to indent from right of page. Default is 20 pixels.
Top	Enter number of units from top of page to start printing.
Bottom	Enter the minimum number of units from bottom of page to leave blank.
Typographic Point Size	A typographic point is normally defined as 1/72 inch, but OC://WebConnect Pro allows you to modify this definition. This feature allows fine-grained scaling of print output, as might be required for fitting the output to a preprinted form.
Points Per Inch (horizontal)	Enter a number of horizontal points per inch to define a typographic point.
Points Per Inch (vertical)	Enter the number of vertical points per inch to define a typographic point.

☞

Troubleshooting

If the print method chosen is not supported by the browser or has not been installed or enabled on the browser platform, error messages might display.

For more information about OC://WebConnect Pro printing solutions, see *Chapter 17: OC://WebConnect Pro Print Solutions.*

Chapter 9: Configuring VT Emulation Sessions

Overview

OC://WebConnect Pro combines a feature-rich, VT Java emulation client with centralized configuration and administration on the server.

Client interface features include keyboard, color, and attribute mapping; copy and paste; and screen print. All emulation sessions can be protected by either RSA's RC4 encryption or SSL authentication and encryption.

Session configuration is provided via centralized configuration and administration tools that can be accessed remotely through a browser. OC://WebConnect Pro provides two methods to configure OC://WebConnect Pro emulation sessions:

- The HTML configuration is a series of HTML pages that access the OC://WebConnect Pro server via a common gateway interface (CGI) interface to create, modify, and delete emulation session configurations via a browser. The HTML Configuration does not require a Java-enabled browser.
- The graphical **GUI Configurator** is a Java applet downloaded to the browser platform and executed via a Java-enabled (JDK 1.1) browser.

Both configuration tools provide full-featured, remote session configuration to create, delete, and modify emulation sessions. An OC://WebConnect Pro server administrator can control important session configuration and management features like host access, security, session negotiation rules, and emulation interface configuration. If desired, the end user can be allowed to configure the keyboard, color, and attribute mapping.

Configuring VT Sessions Using HTML

The OC://WebConnect Pro HTML configuration is a series of HTML pages that retrieve the current server and session information from the OC://WebConnect Pro server through an administrative connection. An administrator can modify server settings and create, modify, or delete emulation session settings. The OC://WebConnect Pro server must be active to use the HTML configuration utility. See *Chapter 2: Starting OC://WebConnect Pro*.

Accessing the VT HTML Session Configuration Page

1. Connect to the OC://WebConnect Pro HTTP Web server: In the URL of a browser, type the following:

   - The host name where the OC://WebConnect Pro HTTP Web server is running

   - The TCP port number

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

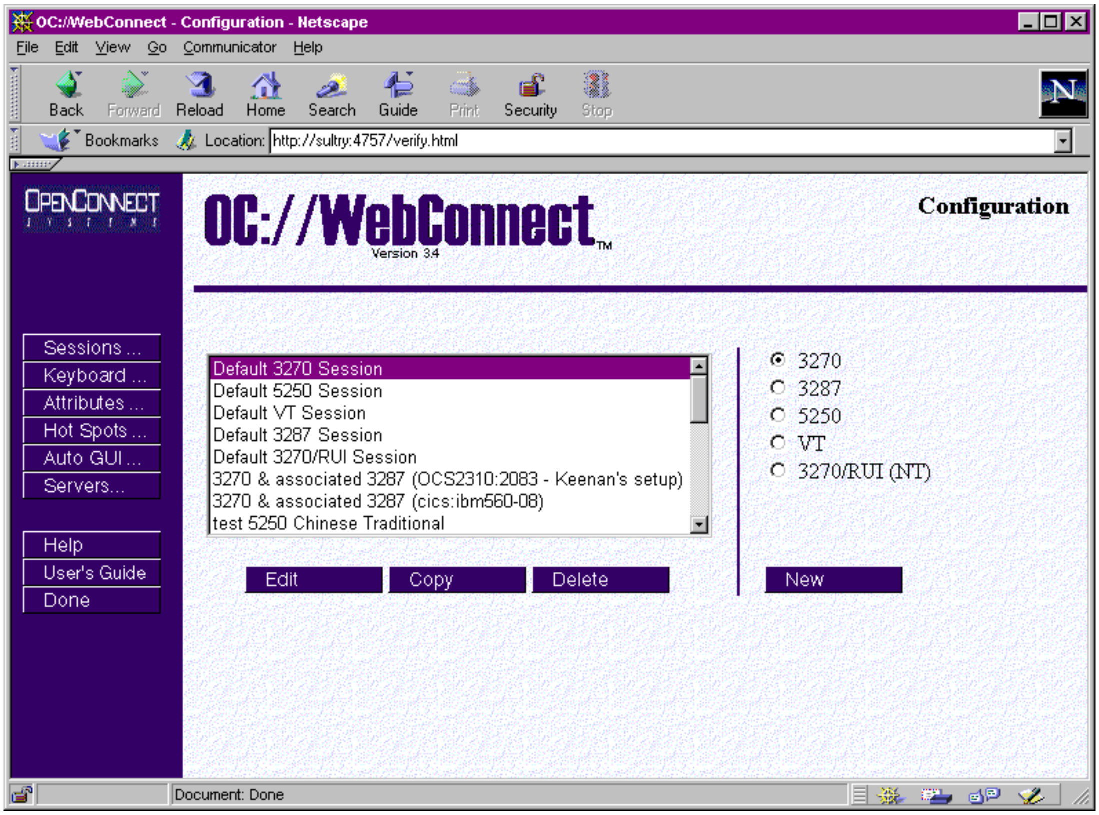
2. Press **Enter**. The **Start Sessions** page is displayed.

3. Click **Configuration** on the left of the **Start Sessions** page. A prompt appears for the **Administrator Password.**

4. Type the password in the box under **Enter Administrator Password** and click **OK**.

   ☞ **Note:** The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

   When the correct administrator password is entered, the main **Configuration** HTML page is displayed.



Location: http://sultry:4757/verify.html

Default 3270 Session
Default 5250 Session
Default VT Session
Default 3287 Session
Default 3270/RUI Session
3270 & associated 3287 (OCS2310:2083 - Keenan's setup)
3270 & associated 3287 (cics:ibm560-08)
test 5250 Chinese Traditional

● 3270
○ 3287
○ 5250
○ VT
○ 3270/RUI (NT)

The main **Configuration** page has three sections:

- At the top is the header section, which shows the OC://WebConnect Pro version and the name of the HTML page displayed, **Configuration** in this example.

- On the left are navigation buttons used to access other OC://WebConnect Pro HTML pages for context-sensitive **Help**, the online **User's Guide**, and configuration pages for mapping other OC://WebConnect Pro features. The **Done** button exits this page.

- To the middle and right is the session configuration section used to create, edit, or delete session configurations.

Navigation Buttons

Sessions – Configure an individual session configuration. This page is displayed first.

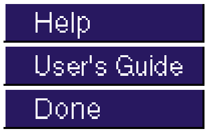
Keyboard – Create, modify, or delete a keyboard map.

Attributes – Create, modify, or delete an attribute and color map.

Hot Spots – Create, modify, or delete a hot spot map.

Auto GUI – Create, modify, or delete an auto GUI map.

Servers – Modify server settings.



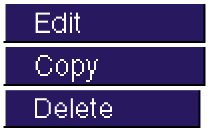
Access context-sensitive help.

Access online user guide.

Exit session configuration.

Session Configuration Buttons

A list of existing session configurations is displayed. To edit, copy, or delete an existing session, select a session and click the appropriate button.



Edit an existing session configuration.

Create a new session configuration from an existing session configuration.

Delete an existing session configuration.

A group of radio buttons indicates the supported emulation types. To create a new session configuration, choose an emulation type, and then click **New**.

Create a new session configuration.

Configuring a New VT Session Using HTML

1. Click the **VT** radio button.
2. Click **New**. A new session configuration page, **Description**, appears with the *default* session settings.
3. Type a unique session description and file name (without an extension).
4. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **VT**, **Display**, and **Printing**. Modify the settings as needed.

☞

> **More Information**
>
> For more information about VT emulation features, see “VT Emulation Session Features and Settings” in this chapter.

5. To save the new VT session configuration, click **Save** on the sidebar.

   -or-

   To abort the creation of a new VT session configuration, click **Cancel** on the sidebar.

Editing an Existing VT Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Edit**. The first session configuration page appears with the chosen session description.
3. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **VT**, **Display**, and **Printing**. Modify the settings as needed.

☞

> **More Information**
>
> For more information about VT emulation features, see “VT Emulation Session Features and Settings” in this chapter.

4. To save the changes, click **Save** on the sidebar.

   -or-

   To cancel the changes made to an existing VT session configuration, click **Cancel** on the sidebar.

Copying an Existing VT Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Copy**. A new session configuration page appears with the same session settings.
3. Type a unique session description and file name.
4. Step through the buttons on the left to access other sections of session configuration information—**Network**, **Security**, **Telnet**, **VT**, **Display**, and **Printing**. Modify the settings as needed.

> **More Information**
>
> For more information about VT emulation features, see “VT Emulation Session Features and Settings” in this chapter.

5. To save the new VT session configuration, click **Save** on the sidebar.

   -or-

   To cancel the creation of a new VT session configuration, click **Cancel** on the sidebar.

Deleting an Existing VT Session Configuration Using HTML

1. Select an existing session configuration.
2. Click **Delete**. A new page appears requesting you to confirm the deletion.
3. Click **Delete** again to delete the selected session.

   -or-

   Click **Cancel** to stop the deletion.

> **Note:** Default session configurations cannot be deleted.

Configuring VT Sessions Using the GUI Configurator

After the OC://WebConnect Pro server is started (see *Chapter 2: Starting OC://WebConnect Pro*), you can access the GUI Configurator applet by selecting **GUI Config** on any OC://*WebConnect Pro* HTML page using a JDK 1.1 Java-enabled browser.

☞ **More Information**

You can restrict access to the GUI Configurator applet by removing the button from any OC://*WebConnect Pro* HTML page, or you can create custom HTML access to the GUI Configurator applet. See *Chapter 12: Customizing OC://WebConnect Pro*.

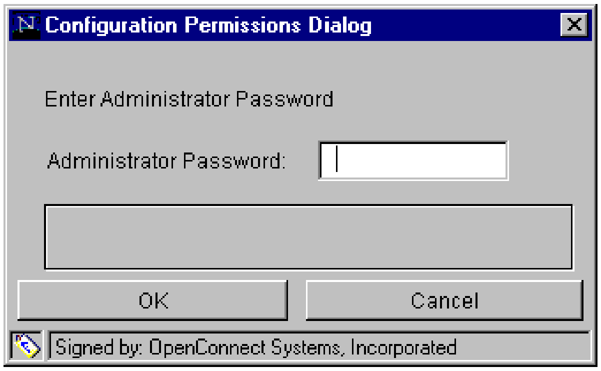
Accessing the GUI Configurator for VT Session Configuration

1. Start the OC://WebConnect Pro server. (See *Chapter 2: Starting OC://WebConnect Pro*.)

2. From any OC://WebConnect Pro HTML page using a JDK 1.1 Java-enabled browser, click **GUI Config** on the sidebar. The browser downloads and starts the GUI Configurator applet.

   You might see one or more Java permissions windows. Click **Grant** in each window to authorize the applet to run.

   After the applet starts, the **Configuration Permissions Dialog** window displays asking for the administrator password.

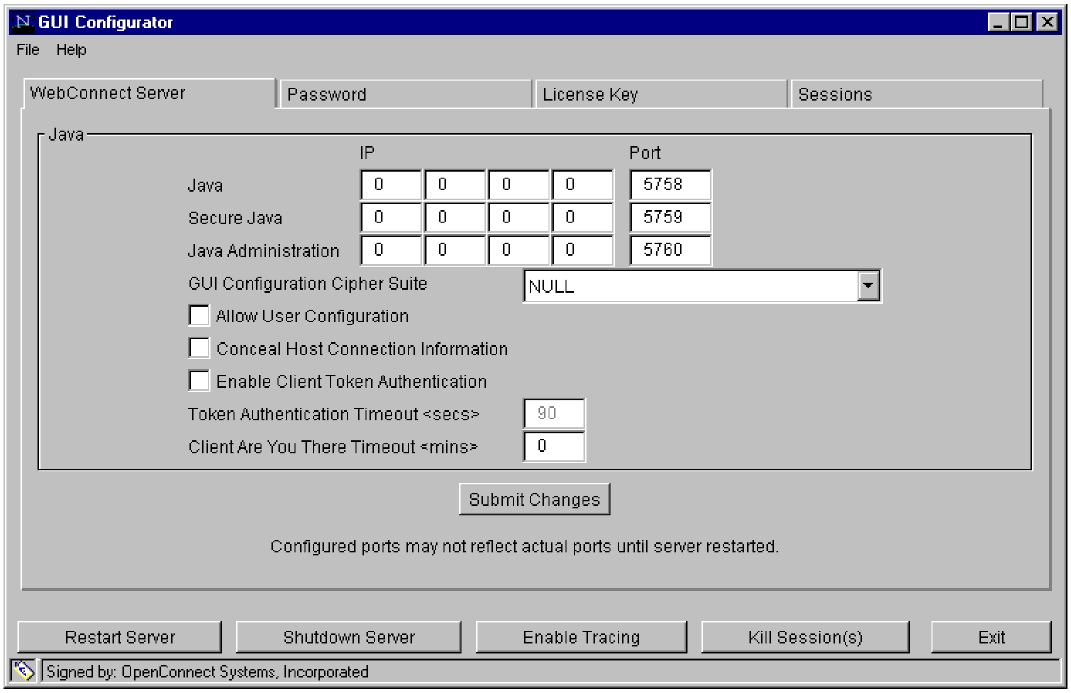


Configuration Permissions Dialog
Enter Administrator Password
Administrator Password:
OK
Cancel
Signed by: OpenConnect Systems, Incorporated

3. Type the password in the **Administrator Password** field and click **OK**.

☞ **Note:** The default password is **OCS** (uppercase). Because this password is documented, it is recommended that you change the administrator password.

When the correct administrator password is entered, the OC://WebConnect Pro **GUI Configurator** window, shown below, opens:



Java

	IP				Port
Java	0	0	0	0	5758
Secure Java	0	0	0	0	5759
Java Administration	0	0	0	0	5760

GUI Configuration Cipher Suite: NULL

□ Allow User Configuration

□ Conceal Host Connection Information

□ Enable Client Token Authentication

Token Authentication Timeout <secs> 90

Client Are You There Timeout <mins> 0

Configured ports may not reflect actual ports until server restarted.

Signed by: OpenConnect Systems, Incorporated

The window has four tabs at the top. The tab currently selected is **Server**.

☞

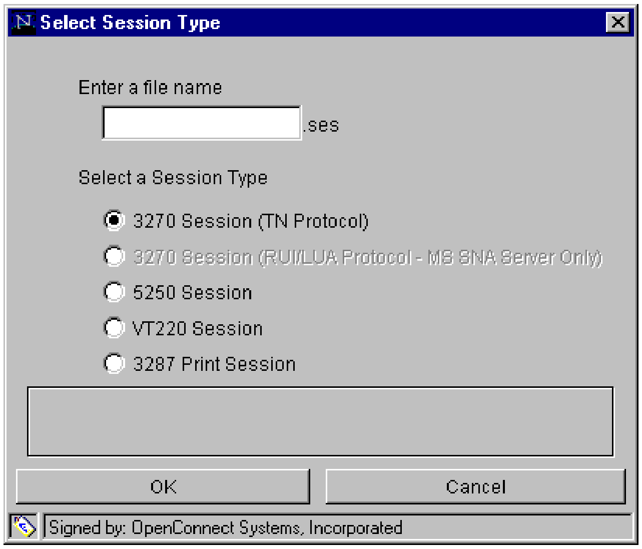
More Information

For more information on the OC://WebConnect Pro **Server**, **Password**, and **License Key** tabs, see *Chapter 5: Server Configuration and Administration.*

Configuring a New VT Emulation Session

1. Click the **Sessions** tab on the OC://WebConnect Pro **GUI Configurator** window. A list of defined sessions displays.

2. Click **Create**. The **Select Session Type** window displays.



Select Session Type

Enter a file name

[   ] .ses

Select a Session Type

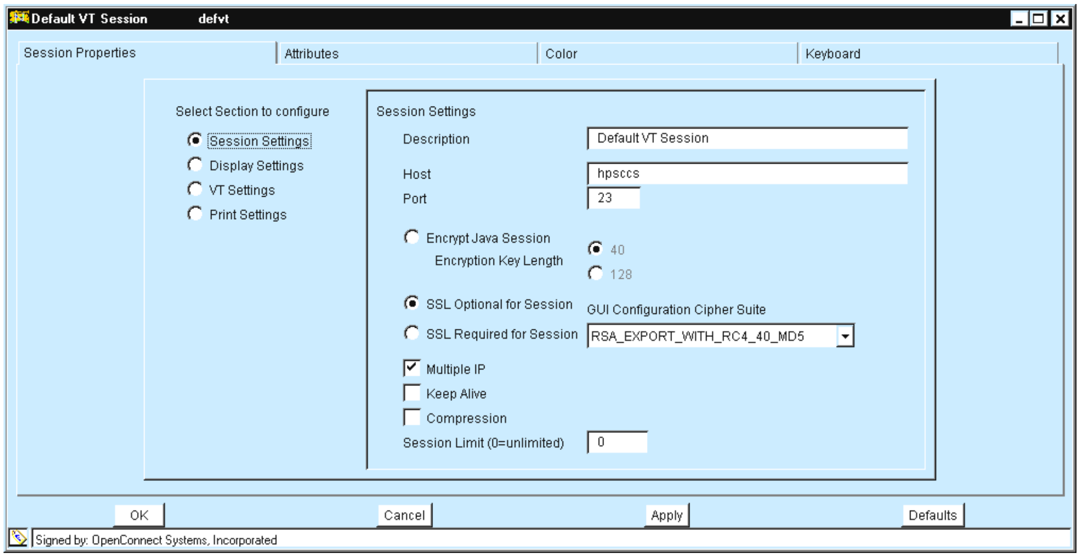
- ● 3270 Session (TN Protocol)
- ○ 3270 Session (RUI/LUA Protocol - MS SNA Server Only)
- ○ 5250 Session
- ○ VT220 Session
- ○ 3287 Print Session

3. Type a unique file name (without an extension) for the new session.

Notes

- When choosing a file name for a session configuration, consider that files are listed on the **Sessions** window in alphabetical order.
- To restore the form to default display values, select the **Defaults** button.

4. Select **VT220 Session** and click **OK**. The **GUI Configurator** displays the **Session Properties** window for the selected emulator type.



Default VT Session defvt

Select Section to configure

- ● Session Settings
- ○ Display Settings
- ○ VT Settings
- ○ Print Settings

Session Settings

Description: Default VT Session

Host: hpsccs

Port: 23

○ Encrypt Java Session

Encryption Key Length: ● 40 ○ 128

● SSL Optional for Session

○ SSL Required for Session

GUI Configuration Cipher Suite: RSA_EXPORT_WITH_RC4_40_MD5

☑ Multiple IP

☐ Keep Alive

☐ Compression

Session Limit (0=unlimited): 0

5. Modify **Session Settings** options as needed on the **Session Properties** window.
6. Click each radio button and modify settings if necessary:
    - **Display Settings**
    - **VT Settings**
    - **Print Settings**
7. Now, step through the other tabs—**Attributes**, **Color**, and **Keyboard**—modifying settings as needed.

☞

> **Notes**
>
> For more information about VT emulation features, see “VT Emulation Session Features and Settings” in this chapter.
>
> The tabs displayed depend on the mode the configuration applet is in and the emulation type of the session selected. For example, if the applet is in user mode, the **Sessions Properties** tab does not display.

8. Click **OK** to save the session configuration to a session (***.ses**) file.

    -or-

    Click **Cancel** to abort creating the new session.

Editing a VT Session Configuration

1. Click the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to edit and click **Properties**. The **GUI Configurator** displays the **Session Properties** window for the selected emulation type.
3. Modify **Session Settings** options as needed on the **Session Properties** window.
4. Click each radio button and modify settings if necessary:
    - **Display Settings**
    - **VT Settings**
    - **Print Settings**
5. Now, step through the other tabs—**Attributes**, **Color**, and **Keyboard**—modifying settings as needed.

More Information

For more information about VT emulation features, see “VT Emulation Session Features and Settings” in this chapter.

6. Click **OK** to save the session configuration to a session (***.ses**) file.

   -or-

   Click **Cancel** to abort saving the changes.

Deleting a VT Emulation Session Configuration

1. Choose the **Session** tab on the OC://WebConnect Pro **GUI Configurator** window.
2. Select the session configuration to delete and click **Delete**. A window is displayed requesting confirmation of the delete.
3. Click **OK** to confirm the deletion. The session file is deleted.

Note: Default session files cannot be deleted.

VT Emulation Features and Settings

Description

Field	Procedure
Description	Type a brief description for the session configuration. This description appears on windows used to select a session to start, modify, or delete.
Save as	Type a unique file name, without an extension, in which to store the emulation session settings.

VT Network Settings

Field	Procedure
Connect to host	Enter the host name of the destination system. This can be the TCP/IP host name of the UNIX system to access.
Port	Enter the TCP/IP port number the UNIX system uses for emulation connections. The default Telnet port number is **23**.
Enable TCP/IP Keep Alive	Enable this option for OC://WebConnect Pro to utilize the Keep Alive feature of the underlying TCP/IP stack to monitor and clean up after unexpected session outages, such as PC client power losses or cable faults. Keep Alive monitors the connection from the browser client to the OC://WebConnect Pro server, as well as the connection from the OC://WebConnect Pro server to the UNIX system.
Try Multiple IP addresses	Enable this option if the host name being used for host connectivity refers to multiple DNS addresses. Multiple DNS addresses provide the OC://WebConnect Pro server a choice of Telnet servers when a server is busy or the session type is not available. **Note:** If this option is not enabled, only one connection attempt—to the first IP address returned—is made. OC://WebConnect Pro evaluates the DNS addresses serially to make a host connection, depending on the Telnet server used. Example: Host XY is configured for two IP addresses (Telnet server X and Telnet server Y). OC://WebConnect Pro wants a Telnet server, and Telnet server X is in use. OC://WebConnect Pro automatically attempts to connect to Telnet server Y.
Enable data compression	Enable this option to compress data flowing between the OC://WebConnect Pro server and the Java client. **Note:** The tradeoff for decreased network traffic is time spent compressing and decompressing data.

Security Settings

Field	Procedure
Diffie-Hellman/RC4 encryption	Enable this option to encrypt session data between the OC://WebConnect Pro server and Java client session. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both.
Key Length	Select **40 bits** or **128 bits**. 128-bit encryption is available only in the US. If 128-bit encryption is selected for a non-US version, the session defaults to 40-bit encryption. The encryption method for a specific emulation can be seen by selecting **Help**>**Help Desk**. **Note:** Key length in Ultra Lite session is always **40 bits**.
SSL	Enable SSL (Secure Socket Layer) to use an SSL cipher suite for authentication and/or encryption of data between the OC://WebConnect Pro server and the Java client session. This option requires that the OC://WebConnect Pro server Secure Java Port is configured and active. See *Chapter 5: Server Configuration and Administration* for more information about the Secure Java Port. Either **Diffie-Hellman/RC4 encryption** or **SSL** can be selected, but not both. Select **Optional** to allow emulation client users to choose SSL or not. Select **Required** to force the use of SSL session configuration.
SSL Cipher Suite	Select an SSL Cipher Suite based on the level of security desired.
Limit number of sessions per applet	Enable this option to restrict the number of new sessions that can be started from an emulation session already connected. Each Java emulation client has a **File**>**New** menu item, which allows a new emulation session to be spawned from the existing connection. By default, an emulation client user can start as many sessions as the OC://WebConnect Pro license key allows.
sessions per applet	Specify the number of sessions that can be spawned from an emulation applet. Zero disables this option.

☞

More Information

For more information about OC://WebConnect Pro security features, see *Chapter 15: Security Overview*.

Display Settings

Field	Procedure
Language	Select the language to use for messages in the VT session emulation applet window.
Code Page	Enter the number of the code page for the target host application. Values range from 37 to 61712.
Transform Type	Select the code page transform type from the list box. **Note:** If using the Single/Double Byte EBCDIC-to-Unicode option, the ability to switch the single-byte code pages using a default key is available.
Clickpad	Enable this option to initially show a clickpad in an applet window. The clickpad can be used to select function keys or other special keys not mapped to the local keyboard..
Font Size	Enter the number for the default font point size to use for text displayed in the applet window. This font size dictates the initial client window size.
Keyboard Map	Enter the keyboard map (**.kbm)** file name for the session being edited. The default is **defvt.kbm**.
Attribute Map	Enter the **.atm** file name for the session being edited. The default is **defvt.atm**.

☞

> **More Information**
>
> For more information about mapping user interface and display options, see *Chapter 10: Display Options Configuration and Features*.

VT Settings

Field	Procedure
Lines	Click the down arrow and select the number of rows (lines) to display.
Columns	Click the down arrow and select the number of columns to display.
Tabs	Specify the tab settings by typing a T in each line position where a tab is desired.
Auto Wrap	Click the check box to automatically wrap to the next line text that exceeds the line length.
Margin Bell	Click the check box to activate the margin bell. The warning bell sounds when the cursor is moved within eight characters of the end of line, based on the number of columns set.

Printing Settings

Field	Procedure
Radio buttons:	Select one.
Disabled	Select this option to disable screen print for this VT session.
OC://WebPrint	Select this option to use OC://WebPrint (Windows platform only) for screen print. OC://WebPrint must be installed on the browser platform to use this solution. This option is supported on JDK 1.0 and greater browsers. The OC://WebPrint print solution is available in all OC://WebConnect Pro applets and avoids some problems associated with JDK 1.1 printing by printing at the resolution of the underlying print driver. OC://WebPrint prints to any paper size reported by the printer driver and honors all session settings and formatting controls from the data stream, generating uniformly spaced print output. In addition, OC://WebPrint supports two features not supported by the other print solutions: • A raw mode of operation that allows printer-specific codes to be passed in the data stream. • A suppress-printer-dialog option to allow jobs to be sent directly to the default printer without user intervention.
JavaScript	Select this option to use JavaScript, which is supported in some JDK 1.0 and greater browsers. The JavaScript print solution is supported by all OC://WebConnect Pro emulation applets. JavaScript functions are downloaded to the PC as part of the HTML page that loads the emulation applet. Therefore, if you write an HTML page to load the applet, the page must include JavaScript print functions to prevent breaking the JavaScript print solution. When printing with the JavaScript print solution, the JavaScript opens a separate browser window, writes the print output to that window, and then sends the browser contents to the system printer as if the user selected **File**>**Print** from the browser menu. JavaScript printing is convenient and provides a good print solution for applications not requiring control of the output format. Because the print output is rendered through the browser, the browser is in charge of formatting, and virtually all session settings and data stream commands related to formatting are ignored.
JDK 1.1 Print	Select this option for screen print using JDK 1.1 print methods embedded in JDK 1.1-based browsers. The JDK 1.1 print solution is the native print implementation provided by all browsers utilizing JDK 1.1 or later, making it available when using an Enhanced or Power User applet. The browser’s JVM (Java

Field	Procedure
	Virtual Machine) implementing JDK 1.1 printing prints at a fixed resolution, typically 72 or 96 pixels per inch, which is usually less than the resolution of the attached printer. This mismatch causes incompatibilities with the **Windows Generic/Text Only** driver and can cause nonuniform character spacing when attempting to print at specified line and/or character densities. Printing with the **Auto Fit** feature enabled prevents the latter problem. **Note:** Screen printing always prints in **Auto Fit** mode. Early versions of JDK 1.1 implemented in most browsers contain bugs that affect the ability of OC://WebConnect Pro to properly determine the page size. In these older browsers, the page size is assumed to be 8.5-by-11-inch paper in portrait mode. As of JDK 1.1.4, most of these bugs have been fixed, allowing support of landscape mode and other paper sizes.
Suppress Printer Dialog (OC://WebPrint only)	Enable this option to bypass the system print dialog when a print request is made. This feature allows jobs to be sent directly to the default printer without user intervention and is supported only by the OC://WebPrint print solution.
Character Mode	Select this option to send one character at a time to a printer, allowing precise control of spacing and printing of attributes. By default, printing is performed in line mode, meaning text is sent one line at a time to the printer driver. In line mode, character spacing is determined by the printer driver and the selected font, so the right and bottom edges of the printed output are determined by this spacing rather than by margin settings. Attributes and printing to fixed metrics are not supported in line mode. **Note:** Character mode is not supported by the JavaScript print solution.
Margin	Select **Pixels** or typographic **Points** as the unit of measurement for margin settings, which apply to both screen print and 3287 printing. In addition to the potential cosmetic use of this feature, print margin settings can be used to help with form alignment and to prevent data loss near paper edges. If there is no print margin, the print output for certain printers can be truncated near the edge of the paper. Appropriate print margins can be set to remedy the problem. A pixel is a logical unit of measure, specific to the print solution, while a typographic point is a physical unit of measure, normally equal to 1/72 inch. In some cases, it is appropriate to set the margins to 0. When working with the **Windows Generic/Text Only** printer driver, nonzero margins yield unpredictable results. Setting zero margins also allows JDK 1.1 Print to print uniformly, provided the **Typographic Point Size** is set to 72 both horizontally and vertically.
Left	Enter number of units to indent from left of page. Default is 20 pixels.

Field	Procedure
Right	Enter number of units to indent from right of page. Default is 20 pixels.
Top	Enter number of units from top of page to start printing.
Bottom	Enter the minimum number of units from bottom of page to leave blank.
Typographic Point Size	A typographic point is normally defined as 1/72 inch, but OC://WebConnect Pro allows you to modify this definition. This feature allows fine-grained scaling of print output, as might be required for fitting the output to a preprinted form.
Points Per Inch (horizontal)	Enter a number of horizontal points per inch to define a typographic point.
Points Per Inch (vertical)	Enter the number of vertical points per inch to define a typographic point.

☞

Troubleshooting

If the print method chosen is not supported by the browser or has not been installed or enabled on the browser platform, error messages might occur.

For more information about OC://WebConnect Pro printing solutions, see *Chapter 17: OC://WebConnect Pro Print Solutions.*

Chapter 10: Display Options Configuration and Features

Accessing Display Options

This section discusses the display options that can be modified by an administrator or by the user if the administrator has enabled **Allow User Configuration** from the WebConnect Pro tab in the GUI configuration.

When you log on to OC://WebConnect Pro without administrative privileges, you are in user mode. In user mode, you can change display options locally on the browser machine. When you log on with administrative privileges, you are in administrator mode. In administrator mode, all configuration changes, even display options, are made to the server files.

User mode displays a list of defined sessions and a **Properties** button. The **Properties** button displays a configuration window that allows you to view and modify the key, color, attribute, hotspot, and auto GUI map files associated with the selected session. The properties of the session are not available when the configuration applet is in user mode.

Switching from User to Administrator Mode

1. Log on to OC://WebConnect Pro.
2. Click the **Admin Config** button. The **Configuration Permissions Dialog** window displays.
3. Enter the appropriate password in the **Administrator Password** field.
4. Click the **OK** button. The OC://WebConnect Pro configuration applet displays in administrator mode.

Notes

-
  Properties button on the **Sessions** tab on the configuration applet window.
- Changes to display options do not take effect until the *next* time a session is started. That is, if a session is open, the changes do not appear until the session is stopped and restarted.

Setting Auto GUI Options

The **Auto GUI** tab creates a graphical user interface (GUI) to replace host screens. When you enable the **Auto GUI**, your host's "green-on-black" screens are replaced with a GUI containing labels and text fields.

Notes

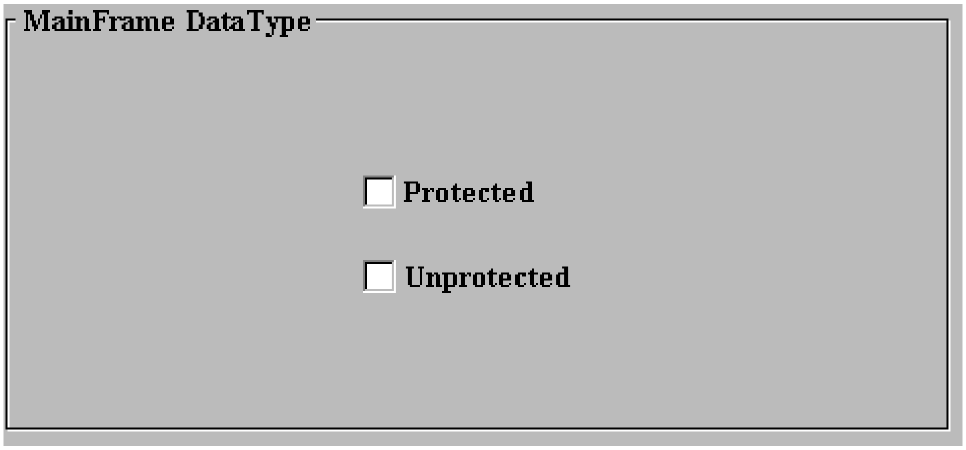
- **Auto GUI** can be configured only by the administrator in administrator mode.
- Screen sizes vary and might blink when using labels and text fields because their components occupy different amounts of space.
- With Java, text fields do not accept colors the same as labels. Therefore, certain colors are not available for text fields.

To set GUI options, follow these steps:

1. Click the **Auto GUI** tab in the OC://WebConnect Pro **GUI Configurator** applet window.

   Note: Auto GUI is available for 3270 and 5250 sessions only.

2. Click the **Protected** or **Unprotected** check box in the **MainFrame Data Type** box. **Protected** assigns options to host fields that cannot be changed or edited. **Unprotected** assigns options to host fields you can change.

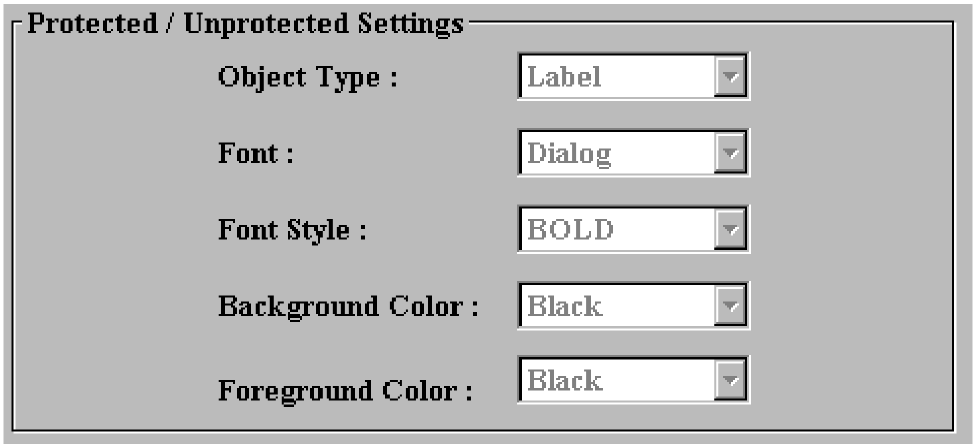


MainFrame DataType

□ Protected

□ Unprotected

☞ **Note:** If you choose **Protected** in the **Mainframe Data Type** box, the **Object Type** field in the **Protected/Unprotected Settings** box automatically displays **Label**. If you choose **Protected** in the **Mainframe Data Type box**, the **Object Type** field in the **Protected/Unprotected Settings** box automatically displays **Text Field**.



Protected / Unprotected Settings

Object Type :	Label
Font :	Dialog
Font Style :	BOLD
Background Color :	Black
Foreground Color :	Black

3. Select a font type from the **Font** list box in the **Protected/Unprotected Settings** box. Font types vary based on your platform.

4. Select a font style from the **Font Style** list box. The choices are **Bold**, **Plain**, and **Italics**.

5. Select a background color from the **Background Color** list box. The choices are **Black**, **Blue**, **Gray**, **Green**, **Magenta**, **Red**, **Turquoise**, **White**, and **Yellow**.

6. Select a foreground color from the **Foreground Color** list box. The choices are **Black**, **Blue**, **Gray**, **Green**, **Magenta**, **Red**, **Turquoise**, **White**, and **Yellow.**

7. Select a font size for the protected and unprotected fields in the **Font Size** list box on the **Main Panel Settings** box.

   The **Auto GUI** settings you choose display in the **Preview Settings** box.

Using the Hotspots Tab

Use the **Hotspots** tab on the OC://WebConnect Pro **GUI Configurator** applet window to map buttons that initiate PF keys. The **Hotspots** tab displays if you are configuring properties for a 3270 or 5250 session.

Setting a Hot Spot

To set a hot spot, follow these steps:

1. In the **Match Text** field in the **Hotspot** box, type the text to display on the button that will map to and initiate an emulator key (such as a PF key).

2. Click in the list box the emulator key you are mapping.

3. Click the **Add Entry** button. The text and emulator key are listed in the **Hotspot Current Settings** box.

4. Choose a button based on the desired action:
   - **OK** saves your changes.
   - **Cancel** exits without saving your changes.
   - **Defaults** deletes your changes and replaces them with default options.
   - **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Note: Hotspots are available for 3270 and 5250 sessions only.

Modifying a Hot Spot

To modify a hot spot, follow these steps:

1. Select **3270** or **5250** from the **Session** menu on the **Hotspots** tab. The hot spot options display for the selected emulation type.
2. Select the text and emulator key entry in the **Hotspot Current Settings** box. The text displays in the **Hotspot Configuration** box, and the emulator key displays in the **Match Text** box.
3. Map the text to another emulation key in the **Match Text** box, or type different text in the **Hotspot Configuration** box to initiate the emulator key.
4. Click **Replace Entry**. The new text and emulator key entry displays in the **Hotspot Current Settings** box.
5. Choose a button based on the desired action:
   - **OK** saves your changes.
   - **Cancel** exits without saving your changes.
   - **Defaults** deletes your changes and replaces them with default options.
   - **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Deleting a Hot Spot

1. Select **3270** or **5250** from the **Session** menu on the **Hotspots** tab. The hot spot options display for the selected emulation type.
2. Click the text and emulator key entry you want to delete in the **HotSpot Current Settings** box.
3. Click **Delete Entry**. The entry is deleted.
4. Choose a button based on the desired action:
   - **OK** saves your changes.
   - **Cancel** exits without saving your changes.
   - **Defaults** deletes your changes and replaces them with default options.
   - **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Displaying Hot Spots

To display hot spots, select the **Hotspots** check box from the **Settings** menu on your emulation screen.

Using the Attributes Tab

Use the **Attributes** tab on the OC://WebConnect Pro **GUI Configurator** applet window to assign display and emulation attributes for host screens.

Many applications use IBM base and extended attributes to identify characters and fields for special functions. Examples of IBM attributes are protected fields (fields that cannot be edited) or blinking text.

The **Attributes** tab lists IBM attributes in the **Application Attributes** list. Emulation attributes displayed by your application can be assigned or mapped to any of the following:

Foreground color (selectable)
Background color (selectable)
Blink
Underline
Reverse video
High intensity
Transparency
Hot spots

OC://WebConnect Pro has default attribute map files (**def3270.atm**, **def5250.atm**, and **defvt.atm**). Each file contains a production-set attribute map. You can use these default attribute maps or change them to suit your needs. You also can save the modified attribute maps to the original default file name or to a new file name.

Mapping Display Attributes

To display the current attribute map for a listed application attribute, follow these steps:

1. Select a session type from the **Session** menu and click the **Properties** button.

☞

> **Notes**
>
> - Each session type (3270, 5250, VT, or 3287) has different application attributes.
> - You must have a session open to view its attributes.

2. Click the **Attributes** tab.
3. Select an application attribute from the **Application Attributes** box. OC://WebConnect Pro shows the display attributes in the **Display Attributes** box.
4. Choose the display attributes desired from the **Display Attributes** box.

5. Choose a button based on the desired action:

   - **OK** saves your changes.
   - **Cancel** exits without saving your changes.
   - **Defaults** deletes your changes and replaces them with default options.
   - **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Application Attribute Considerations

Lightpen attributes. Some host applications use lightpen fields. OC://WebConnect Pro uses production-set parameters to display lightpen-selectable fields in red. All nonselectable fields display in green. However, you can use the **Attributes** tab to map other display attributes to an application's lightpen fields.

Hot spot attributes. You can map display attributes to hot spots. Select the **Hotspot - Selectable** application attribute from the scroll list and map desired display attributes. The hot spots appear with the attributes you map to them.

Display Attribute Considerations

Foreground and background color attributes. You can set the attribute's foreground and background colors and activate other characteristics, such as toggle buttons. When you select foreground and background colors, the **Display Color Sample** line shows a sample of the colors. This representation is the display attribute or the way the application attribute is to appear in the workspace.

Dotted underline attribute. This attribute instructs OC://WebConnect Pro to mark column separators with decimal characters. A decimal character between fields shows the column boundary.

Button attribute. This attribute allows the recognized application attribute to display with bordering similar to a physical key.

Inset attribute. This attribute marks recognized application attributes as buttons "depressed" into the surrounding background.

Using the Color Tab

Colors that appear in the OC://WebConnect Pro workspace are display colors that represent colors specified in the session's data stream. The session's color specifications are emulation colors mapped to the display colors available from your windowing system. The default colors displayed by OC://WebConnect Pro normally allow you to perform the tasks you want. In some cases, however, you might want to map new display colors to particular emulation colors so that information appears in the color you want.

The **Colors** tab shows a list of standard emulation colors. When you select an emulation color name, the display color mapped to the emulation color displays.

When you load a session file into memory, the session's color map file also is loaded. OC://WebConnect Pro automatically opens the color map file referenced in the session file.

OC://WebConnect Pro has default color files (**def3270.clm**, **defvt.clm**, and **def5250.clm**). Each file contains a production-set color map. For example, a color map file can include an emulation color, such as blue, that is mapped to a light blue display color. In this case, OC://WebConnect Pro displays light blue in its workspace when the application specifies blue in the session datastream.

Mapping Colors

During a session, you can replace current colors with new display colors.

1. Select a session type from the **Session** menu on the **Select Session Type** window, and click the **Properties** button.
2. Click the **Colors** tab.

☞

Notes

- You must have a session open to view its attributes.
- You can add a new color or remove a color by selecting **Add Custom Color** or **Remove Custom Color**.

1. Select an emulation color. The emulation color's assigned display color appears in the **Sample Display** box.
2. Select a standard color from the Standard Color list.
3. Choose a button based on the desired action:
    - **OK** saves your changes.
    - **Cancel** exits without saving your changes.

- **Defaults** deletes your changes and replaces them with default options.
- **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Using the Keyboard Tab

Mapping Key Combinations

You can map keys to perform specific actions.

1. Select a session type from the **Session** menu on the **Sessions** menu.
2. Click the **Properties** button.
3. Click the **Keyboard** tab.
4. From the **Action Keys** list box on the **Keyboard** tab, select a key action such as **Tab**.
5. Click in the **Mapped To** list box.
6. Select the key you want to map to that action from the keyboard displayed on the **Keyboard** tab. The sequence displays in the **Mapped To** list box.
   Example: <**Ctrl+Alt+Del**>
7. Click the **Map** button.
8. Repeat Steps 4 through 7 to map additional keys.
9. Choose a button based on the desired action:
   - **OK** saves your changes.
   - **Cancel** exits without saving your changes.
   - **Defaults** deletes your changes and replaces them with default options.
   - **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Notes

- OC://WebConnect Pro saves the key map sequences to the server if you logged in with administrator-level access. If you logged on in user mode, OC://WebConnect Pro saves your key map sequences locally.
- The key map sequences are saved with a **.kbm** extension. The default **.kbm** files for OC://WebConnect Pro are **def3270.kbm**, **def3287.kbm**, **def5250.kbm**, and **defvt.kbm**.
- Although it is not inhibited by the GUI keyboard mapping tool, mapping functions to alphanumeric keys is not allowed. For example, it is not possible to map a 3270 PF4 to the L key on the PC keyboard.

Remapping Keys

To remap keys, follow these steps:

1. Select a session type from the **Session** menu on the **Sessions** tab.
2. Click the **Properties** button.
3. Click the **Keyboard** tab.
4. From the **Keyboard Map Action Keys** list box, select the key action you want to remap.
5. Click the **Unmap** button. The key mapping is removed from the **Mapped To** list box.
6. Select the key that you want mapped to that action on the keyboard displayed on the Keyboard tab. The mapped sequence displays in the **Mapped To** list box.
7. Repeat Steps 4 through 6 to remap additional keys.
8. Click the **Map** button.

9. Choose a button based on the desired action:

   - **OK** saves your changes.
   - **Cancel** exits without saving your changes.
   - **Defaults** deletes your changes and replaces them with default options.
   - **Apply** activates your changes.

Caution

The **Defaults** button eliminates your changes. If you accidentally click **Defaults** and delete your hot spot options, you can restore them by clicking **Cancel**.

If you click **Save** after you accidentally change hot spot options to the default options, you cannot restore your options!

Notes

- OC://WebConnect Pro saves the key map sequences to the server if you logged in with administrator-level access. If you logged on in user mode, OC://WebConnect Pro saves your key map sequences locally.
- The key map sequences are saved with a **.kbm** extension. The default **.kbm** files for OC://WebConnect Pro are **def3270.kbm**, **def3287.kbm**, **def5250.kbm**, and **defvt.kbm**.

Chapter 11: Emulation Client Applet Features and Interface

Overview

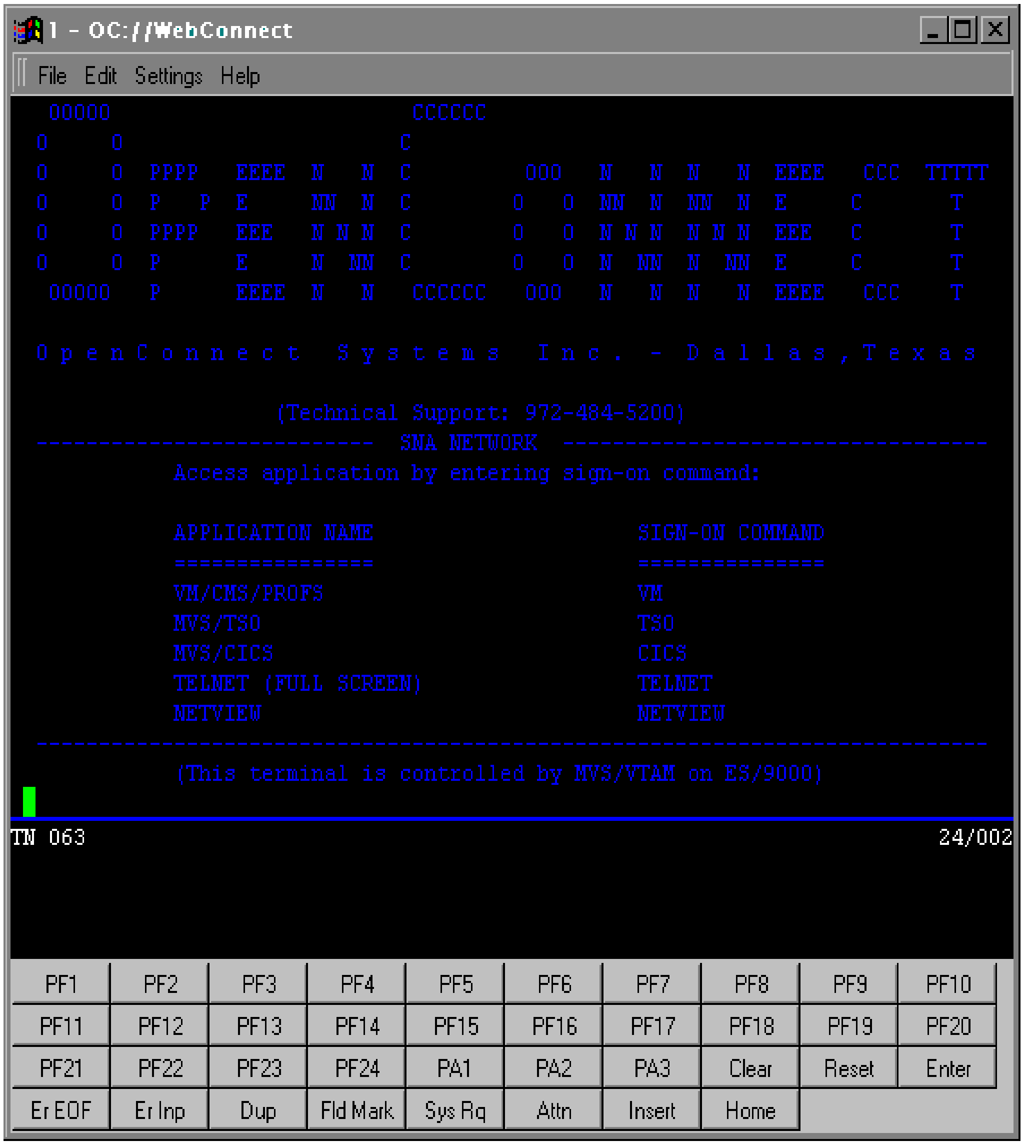
OC://WebConnect Pro includes emulation clients for 3270, 3287, 5250, and VT emulation. The emulation support is provided by the OC://WebConnect Pro emulation server and individual Java emulation client applets. Beyond the basic emulation support, OC://WebConnect Pro applets provide a rich graphical user interface (GUI) to support the end-user features usually provided by a traditional desktop emulation package.

A Java applet is an application program written in Java and executed within a Java-enabled browser interface. Because most of the application user interface is provided by the browser, an applet is fairly small and is ideal for use on the Internet or a corporate intranet.

OC://WebConnect Pro provides three Java emulation client applet packages: **Ultra Lite**, **Enhanced,** and **Power User**. The packages are grouped according to browser support and feature sets.

3270, 5250, and VT Emulation Client User Interface Features

The 3270, 5250, and VT emulation client applets have similar user interfaces and share many user interface features. The client window is made up of a menu bar, emulation space, and an optional clickpad. The menu options provide a variety of features from the ability to spawn a new applet to help. The emulation space displays information as a host connection is being made and is the area in which the host data is presented. The clickpad is a group of buttons to give mouse access to emulation functions. The interface features are explained below.



```
 00000                        CCCCCC
0     0                      C
0     0  PPPP   EEEE  N   N  C         000   N   N  N   N  EEEE   CCC  TTTTT
0     0  P   P  E     NN  N  C        0   0  NN  N  NN  N  E     C       T
0     0  PPPP   EEE   N N N  C        0   0  N N N  N N N  EEE   C       T
0     0  P      E     N  NN  C        0   0  N  NN  N  NN  E     C       T
 00000   P      EEEE  N   N   CCCCCC   000   N   N  N   N  EEEE   CCC    T

OpenConnect Systems Inc. - Dallas,Texas

                   (Technical Support: 972-484-5200)
---------------------------  SNA NETWORK  ----------------------------------
           Access application by entering sign-on command:

           APPLICATION NAME                     SIGN-ON COMMAND
           ================                     ===============
           VM/CMS/PROFS                         VM
           MVS/TSO                              TSO
           MVS/CICS                             CICS
           TELNET (FULL SCREEN)                 TELNET
           NETVIEW                              NETVIEW
----------------------------------------------------------------------------
           (This terminal is controlled by MVS/VTAM on ES/9000)

TN 063                                                                24/002
```

File Menu	Description
New	Spawns another Java emulation session from the current session. The applet is downloaded again. This option can be limited through the session configuration option **Limit number of sessions per applet**.
Print	Prints locally the emulation screen. The screen print functionality is provided through one of three methods: • OC://WebPrint installed on a Java-enabled browser at JDK 1.0 or greater. • **JavaScrip**t included with some browsers. • **JDK 1.1** print functionality included with JDK 1.1-enabled browsers. **Ultra Lite** supports only **OC://Webprint** and **JavaScript.** **Enhanced** and **Power User** support all three print solutions.
File transfer	*Available only with the 3270* **Power User** *applet.* options Allows the end user to send and receive files, using **IND$FILE** or **APVUFILE** file transfer, between the S/390 host and the browser system.
Associated Print Session	Spawns a 3287 print session from a 3270 emulation session. The 3287 session options are configured in the 3270 session configuration.
Exit	Terminates the connection to the host and quits the applet. As long as the browser task is still running, the applet might still be cached by the browser and not need to be downloaded again from the server.

Edit Menu	Description
Copy	Allows the end user to mark a stream of host text and copy it to the system clipboard. This functionality is provided by one of two methods: • OC://Webprint installed on an JDK 1.0 or greater Java-enabled browser • JDK 1.1 copy/paste functionality included with a JDK 1.1-Java enabled browser.
Paste	Allows the end user to paste text, in the system clipboard, to the emulation area or to any other clipboard-enabled window. Example: Copy text from an emulation session to Windows Wordpad. This functionality is provided by one of two methods: • OC://Webprint installed on a JDK 1.0 or greater Java-enabled browser. • JDK 1.1 copy/paste functionality included with a JDK 1.1 Java-enabled browser.

Setting Menu	Description
ClickPad	Displays a group of buttons at the bottom of an emulation screen. The end user can click a button to send an emulation aid key like **Enter**, **F1**, or **F2** to the host. The initial display of the clickpad is controlled via a session configuration setting. While the applet is running, the end user can use this menu option to display or hide the clickpad.
Show printer dialog	*Available with OC://WebPrint only*. Instructs the applet to display a dialog when a print job is created allowing the end user to choose a printer, select landscape or portrait, etc. If this option is not enabled, the print job is sent to the default printer in portrait mode.
HotSpots	*Available only with 3270 and 5250* **Enhanced** *and* **Power User** *applets*. Allows the end user to enable the display of a hot spot button over text that has been defined as a hot spot. The end user can then use a mouse to send the aid key associated with that string of text. See *Chapter 10: Display Options Configuration and Features* for more details.
GUI Screen	*When configured, available only with 3270 and 5250* **Power User** *applets*. Instructs the applet to automatically render the emulation screen to a graphical look and feel.

Font Menu	Description
Font point sizes	*Available only with* **Ultra Lite** *applet*. Allows end users to change the font size used for the emulation text and the size of the applet window. The initial font and window size are determined from the session configuration.

Help Menu	Description
Help desk	Displays emulation, session, security, and connection information. The display of host information can be limited by the OC://WebConnect Pro server setting **Suppress Host Information**.
Key map	Displays the current key mapping of browser platform keys to emulation functions.
Java Logging	*Available only with* **Ultra Lite** *applet*. Writes Java messages to the browser’s Java console. This option can be used for debugging.
About	Displays the applet type and version number.

Emulation Space	Description
Connection messages	Messages are written to the emulation space detailing attempts to connect to the OC://WebConnect Pro server and to the S/390 host.
Security messages	When encryption is used, messages about the generation of encryption keys are written to the emulation space.
Host data	After a host connection is established, host data is displayed in the emulation space of the applet window. The data is displayed according to host data attributes unless **Hotspots** or **AutoGUI** is active.

Feature	Description
Window resizing	The **Enhanced** and **Power User** applets allow the client window to be resized by a mouse click and drag along the applet borders. When the applet window is resized, the font changes to best fit the session window.

☞

More Information

For more information about session configuration, creation, deletion, or modification, refer to one of the following chapters:

- *Chapter 6: Configuring 3270 Emulation Sessions*
- *Chapter 7: Configuring 5250 Emulation Sessions*
- *Chapter 8: Configuring 3287 Print Emulation Sessions*
- *Chapter 9: Configuring VT Emulation Sessions*

3287 User Interface Features

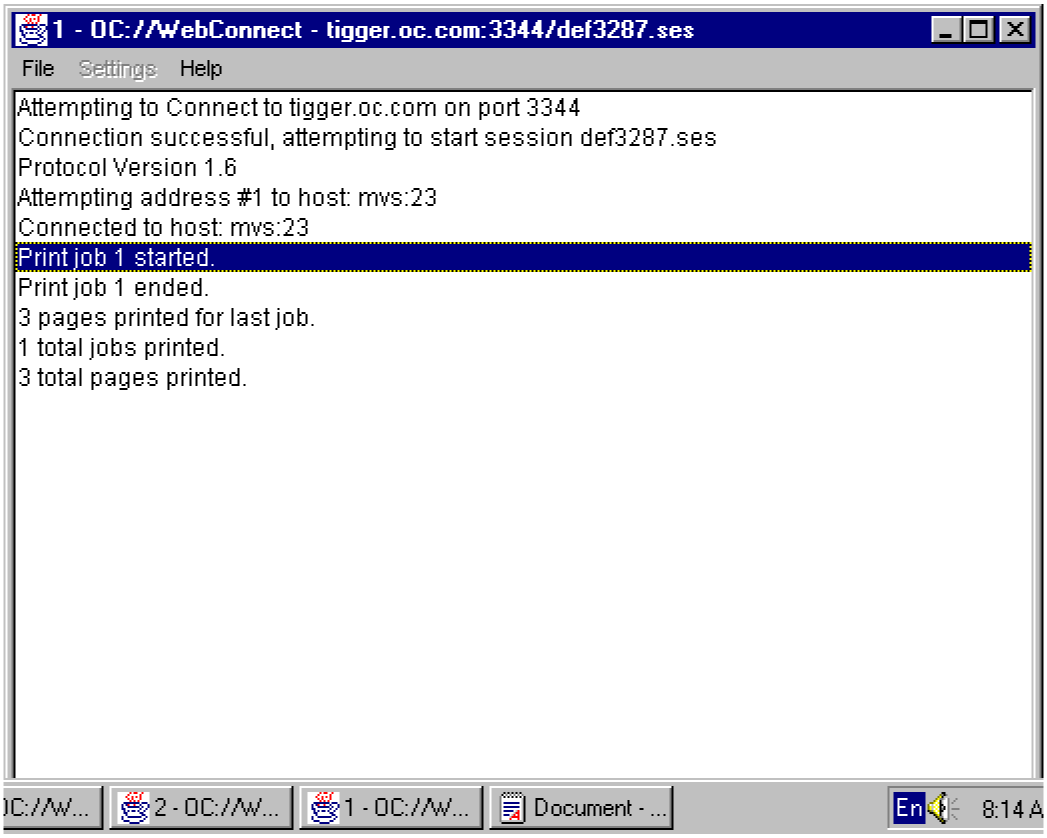
The 3287 session user interface is a simple dialog that displays the progress of 3287 print jobs. A few user options can affect the printed output. These options, as well as other user interface features, are explained below.

FileMenu	Description
Exit	Terminates the connection to the host and quits the the applet. As long as the browser task is still running, the applet might be cached by the browser and not need to be downloaded again from the server .

Setting Menu	Description
Font Autofit	*Available only with OC://WebPrint*. Instructs the Java applet to compress the font to fit the line of print on the printed paper. This is useful if the print data stream defaults to 132 columns of print, but the data is actually only 80 columns.
Show printer dialog	*Available only with OC://Webprint*. Instructs the applet to display a dialog, when a print job is created, that allows the end user to choose a printer, select landscape or portrait, etc. If this option is not enabled, the print job is sent to the default printer in portrait mode.

Help	Description
Help desk	Displays emulation, session, security, and connection information. The display of host information can be limited by the OC://WebConnect Pro server setting **Suppress Host Information**.
About	Displays the applet type and version number.

Printer Dialog	Description
Connection messages	Messages are written to the 3287 session dialog detailing attempts to connect to the OC://WebConnect Pro server and to the S/390 host.
Security messages	When encryption is used, messages about the generation of encryption keys are written to the 3287 print dialog.
Print job messages	Messages are written to the 3287 session dialog reporting the following information: • The status of a print job, for example, **Started** or **Ended** • The number of print jobs completed • The number of pages printed



```
Attempting to Connect to tigger.oc.com on port 3344
Connection successful, attempting to start session def3287.ses
Protocol Version 1.6
Attempting address #1 to host: mvs:23
Connected to host: mvs:23
Print job 1 started.
Print job 1 ended.
3 pages printed for last job.
1 total jobs printed.
3 total pages printed.
```

☞

More Information

For more about emulation features, see *Chapter 8: Configuring 3287 Print Emulation Sessions*.

Choosing an Emulation Client Applet Package

A Java applet is an application program written in Java and run within a Java-enabled browser interface. Because most of the application user interface is provided by the browser, an applet is fairly small and is ideal for use on the Internet or a corporate intranet.

The selection of the OC://WebConnect Pro emulation client Java applet package to use should be made depending on the browser used, the emulation features needed, and the network environment.

Browser Environment and Java Support

Because OC://WebConnect Pro emulation clients are Java applets, the version of browser used is important in the selection of an applet package. Different browsers and browser versions support different Java features. A Java virtual machine (JVM) is included with all Java-enabled browsers. The version of the JVM dictates which Java features are supported. The level of Java support is sometimes referred to as the level of JDK (Java Development Kit) support. For example, browsers that support only JDK 1.0 features support direct printing and copy/paste, but require a coprocess to accomplish the tasks.

In the case of OC://WebConnect Pro, the Java emulation client **Ultra Lite** applet supports JDK 1.0-enabled browsers. **Enhanced** and **Power User** applets require JDK 1.1-enabled browsers and later.

Applet Feature Sets

OC://WebConnect Pro packages are grouped according to the level of features sets required.

- The **Ultra Lite** packages provide basic emulation, along with print and copy/paste functionality.
- The **Enhanced** applets provide all **Ultra Lite** features, as well as JDK 1.1 direct print, copy/paste, and local configuration files.
- **Power User** applets support all **Ultra Lite** and **Enhanced** features, as well as file transfer and Auto GUI.

3287 is available as both an **Ultra Lite** and an **Enhanced** applet.

Network Environment

The network environment in which OC://WebConnect Pro operates and is accessed affects the decision to choose one applet over another or to use OC://WebConnect Pro security features.

OC://WebConnect Pro applets are downloaded to the browser platform the first time the applet is started during a browser session. When the browser user exits, the browser the applet no longer resides on the browser platform. This allows the administrator to maintain software and software configurations on the server while the client platform is dynamically updated.

Applets that provide more features are larger than applets with fewer features. Because the applets are downloaded, the size of the applet affects the amount of time and network traffic to download that applet. If an end user is on a corporate intranet, the amount of time to download a client emulation applet might not be important. If an end user is connecting to OC://WebConnect Pro via the Internet and has a slow modem connection, the size of the applet might be very important.

The use of OC://WebConnect Pro security features can be a necessity depending on the sensitivity of data accessed and the security of the network used. The use of security features requires encryption key generation and data encryption and decryption. The choice of security features is a speed versus security decision.

If an end user is using the corporate intranet and not accessing sensitive data, RSA or SSL might not be required. If an end user is using the Internet and accessing sensitive corporate data, security might be a necessity.

Questions To Ask

- **What is the end user environment?**

  Browser: What browser does the end user use—a JDK 1.0- or JDK 1.1-enabled browser?

  Language: Does the end user require a single-byte or double-byte client? **Enhanced** or **Power User**?

- **What end user features are needed?**

  What emulation does the end user need—3270, 5250, or VT?

  Is 3287 print a requirement? Use OC://WebPrint, JavaScript, or JDK 1.1 print?

  What emulation features does the end user need—file transfer? **Power User** or not?

  Does the end user need copy/paste functionality—OC://WebPrint or JDK 1.1?

  Does the end user need screen print—OC://WebPrint, JavaScript, or JDK 1.1 print?

  Does the user need to configure key, color, or attribute maps? Allow user configuration?

- **What are the administrative needs?**

  Is security a concern? Is security a paramount concern? RSA, SSL?

  Does the administrator need to limit the number of sessions an end user can start? Or allow the user to choose?

  Does the administrator need to monitor response time? RTM or not?

  Does the administrator need to automatically disconnect defunct sessions, such as Are You There?

- **What is the network environment?**

  Is the end user connecting over the Internet or intranet? Is applet size important?

  Is the time to download the applets important? Is applet size important?

  Is connect time important? Encrypt or not?

  Is the time to send and receive data important? Data compression or not?

☞

More Information

For more information about security features, see *Chapter 15: Security Overview*.

For more information about customizing OC://WebConnect Pro, see *Chapter 12: Customizing OC://WebConnect Pro.*

Browser Support of Applets

Browser Support	Ultra Lite	Enhanced	Power User
Netscape 2.x	Yes	No	No
Netscape 3.x	Yes	No	No
Netscape 4.x	Yes	Yes	Yes
Internet Explorer 3.x	Yes	No	No
Internet Explorer 4.x	Yes	Yes	Yes
HotJava 1.x	Yes	Yes	Yes

Emulation Applet Features

Emulation Support	Ultra Lite	Enhanced	Power User
3270	Yes	Yes	Yes
3270E	Yes	Yes	Yes
5250	Yes	Yes	Yes
VT	Yes	Yes	Yes
3287	Yes, using OC://WebPrint or JavaScript	Yes	Yes

Emulation and Connectivity Features	Ultra Lite	Enhanced	Power User
IND$FILE transfer	No	No	Yes
APVUFILE transfer	No	No	Yes
Associate print	Yes, using OC://WebPrint or JavaScript	Yes, using JDK 1.1 Print, OC://WebPrint, or JavaScript	Yes, using JDK 1.1 Print, OC://WebPrint, or JavaScript
RTM (response time monitoring)	Yes	Yes	Yes
IP PassThru	Yes	Yes	Yes
Multiple IP Address	Yes	Yes	Yes
Keep Alive	Yes	Yes	Yes
Telnet Are You There	Yes	Yes	Yes
Client Are You There	Yes	Yes	Yes
Virtual Gateway Support	Yes	Yes	Yes
Terminal type demotion	Yes	Yes	Yes
Model 2,3,4,5	Yes	Yes	Yes
Configured device names	Yes	Yes	Yes

Print Support	Ultra Lite	Enhanced	Power User
3287 print	Yes, using OC://WebPrint or JavaScript	Yes, using JDK 1.1 Print, OC://WebPrint, or JavaScript	Yes, using JDK 1.1 Print, OC://WebPrint, or JavaScript
Print screen	Yes, using OC://WebPrint or JavaScript	Yes, using JDK 1.1 Print, OC://WebPrint, or JavaScript	Yes, using JDK 1.1 Print, OC://WebPrint, or JavaScript
Print Autofit	No	Yes	Yes

User Interface Features	Ultra Lite	Enhanced	Power User
Font size choice	Yes	No, font changes dynamically when the window is resized	No, font changes dynamically when the window is resized
Window resizing	No, size of window is determined by font size	Yes	Yes
Optional clickpad	Yes	Yes	Yes
Copy/paste	Yes, using OC://Webprint	Yes	Yes
Hot spots	No	Yes	Yes
Auto GUI	No	No	Yes
Keymap display	Yes	Yes	Yes
User-defined key, color, attribute, hot spot, and Auto GUI maps	No	Yes	Yes
Administrator-defined keymap	Yes	Yes	Yes
Administrator-defined color, attribute, and hot spot map	No	Yes	Yes
administrator-defined Auto GUI map	No	No	Yes

Security Features	Ultra Lite	Enhanced	Power User
RC4 40-bit encryption	Yes	Yes	Yes
RC4 128-bit encryption	No	Yes	Yes
SSL server authentication	No	Yes	Yes
Client token authentication	No	Yes	Yes
Limit number of new sessions	Yes	Yes	Yes
Data compression	No	Yes	Yes
Conceal host information	Yes	Yes	Yes

Language Support	Ultra Lite	Enhanced	Power User
Four server languages: English French German Castilian Spanish	Yes	Yes	Yes
Single-byte language client interface and data stream: US English UK English French German Italian Castilian Spanish Swiss German Norwegian Dutch Brazilian Portuguese Swedish Turkish Japanese Chinese (Traditional) Chinese (Simplified) Korean	Yes	Yes	Yes
Double-byte language client interface, keyboard input, and data stream: Chinese (Traditional) Chinese (Simplified) Japanese	No	Yes	Yes
Keyboard input and data stream only: Turkish	No	Yes	Yes

Miscellaneous	Ultra Lite	Enhanced	Power User
TCL Scripting	Yes	Yes	Yes
Java Logging	Yes	Yes	Yes

JDK 1.1 File Access Authority

The **Enhanced** and **Power User** applets use features that are available only when using JDK 1.1 Java-enabled browsers. The features require additional security measures because the applet must access the browser platform's file system.

Security is provided using certificates included with the applets and verified by the browsers. When the browser attempts to execute the applet, it encounters a certificate, delivered with the applet, that details the developer of the applet and the local file system access required. The browser then displays a dialog prompting the user to choose whether to grant the local file system access. If the user chooses to *trust* the applet by granting the access, the applet begins and all functionality is available for use. The browser user can grant the privileges on a temporary or permanent basis. If privileges are granted temporarily, future applet sessions require the user to grant privileges again. If privileges are granted permanently, subsequent downloads and use of the applet are automatically granted privileges. The certificate and privileges can be removed from the browser under the **Security** or **Certificates** section of the browser.

The following OC://WebConnect Pro features require access to the local file system:

- The ability to write to the disk to store user configuration files for key maps, color maps, etc.
- The ability to use the local print spooler for print screens and 3287 print
- The ability to access the local clipboard for copy/paste functionality
- The ability to access the local file system to retrieve and store files for file transfer operations

Chapter 12: Customizing OC://WebConnect Pro

Overview

OC://WebConnect Pro can be easily incorporated into an intranet or Internet Web site to provide the necessary centralized control of feature and host access and provide an easy user interface. The product comes with a default user interface that can be used by both the end user and the administrator in a production environment. In case changes are needed in the interface, the product is designed for easy customization.

The OC://WebConnect Pro product has several pieces, some of which can be modified and some of which can be replaced by a third-party tool. The basic OC://WebConnect Pro product is the OC://WebConnect Pro emulation server and the Java client applets. Additional utilities bring the pieces together and deliver a cohesive product that can be used by the emulation client end users, as well as by the OC://WebConnect Pro administrator. These utilities include the HTML session page, the HTML administration and configuration pages, the GUI Configurator applet, the HTTP server, the CGI interface, and online user's guide. These parts make up the product called OC://WebConnect Pro.

OC://WebConnect Pro User Interface Architecture

The OC://WebConnect Pro default user interface is made up of these sections:

End User Interface

- **Start Sessions** page (**index.html**)
- End user applets (**Ultra Lite**, **Enhanced**, and **Power User**)

Administrator Interface

- Administration – HTML administration pages
- Configuration – HTML configuration pages for server and session configuration
- GUI Configurator – Java applet for server and session configuration

Online Documentation

- User guide – Online *User's Guide and Reference* manual
- Help – Context-sensitive help

End User Interface

Only two sections of the interface are used by the client emulation user (end user):

- The **Start Sessions** page
- The end user applet files

The **Start Sessions** page allows the end user to choose emulation options and download the necessary applet files. The **Start Sessions** page is several HTML files that use a common gateway interface (CGI) utility and macros to list available sessions, give the end user some configuration options, and deliver the applet to the end user's browser. The pages can be customized in many ways. Knowledge of HTML and OC://WebConnect Pro is usually required to customize these pages. Knowledge of JavaScript and CGI allows more extensive customization.

The applet files are the Java client applets that provide the client interface and host connection. The three applet types, **Ultra Lite**, **Enhanced**, and **Power User**, give the end user a choice of feature sets and browser support. Extensive customization of the emulation client interface is available by using OpenVista. Knowledge of Java is required to take advantage of the OpenVista tool.

Administrator Interface

The four remaining sections are used by an OC://WebConnect Pro administrator to configure and administer the OC://WebConnect Pro server and clients.

The user HTML and client applet interfaces can be customized in many ways. It is not recommended that the administrator features be customized.

Customization Ideas

The main reason OC://WebConnect Pro has well-defined pieces is to allow customization. Except for the OC://WebConnect Pro emulation server, all the pieces could be replaced. It is recommended, though, that some pieces like the configuration tools not be replaced.

Some ideas for customization are listed below:

- Make a link to the OC://WebConnect Pro URL from a corporate Web page.
- Make the initial OC://WebConnect Pro HTML page a user page only. Split the end user interface and the administrator interface; that is, remove end user access to the administrative and configuration options.
- Change the look and feel of the **Start Sessions** page (**index.html**) to fit the existing corporate Web pages.
- Add or remove the end user configuration options when starting an emulation session.
- Identify the applet choices by browser requirements.
- Set up the user interface by department.
- Use a CGI script to assign specific (“nail down”) 3287 LUs for printing.
- Deliver different applets with different security options to different user groups.
- Allow the end user to select the LU to which to connect.
- Allow the end user to enter a user ID and choose the session configuration, applet type, and security by user ID.
- Add or remove an emulation client menu option.
- Replace the emulation client interface green screen with a custom graphical interface.
- Replace the host application interface with a simpler graphical interface.
- Replace the emulation client interface with a client interface that combines multiple data sources by using OpenVista development tool.

Customization Tools

Extensive customization can be done with HTML. Combined with the **cgiinfo** utility provided with OC://WebConnect Pro, the product can be cleanly integrated into corporate Web pages and easily maintained through the dynamic HTML provided by the **cgiinfo** utility. Additional tools include JavaScript, CGI scripts, OpenVista, and other Java tools.

Customizing the HTML Interface

The default HTML interface provided with OC://WebConnect Pro combines both the administrator and end user interface. It is provided primarily for demonstration, but can be used as is in a production environment. The default HTML interface takes full advantage of the **cgiinfo** utility and macros to provide the current interface with the current server and session configuration information.

Default HTML Files

The HTML **Sessions** page is the main **index.html** file, which is organized into four frames made up of four different HTML files. In addition to the pages that make up the **Sessions** page, **tclient.html** serves as a template for the dynamic HTML created to start an applet. These files are located in the OC://WebConnect Pro **html** directory.

- **index.html** is the main interface for both end users and administrators. This file is displayed when a user contacts OC://WebConnect Pro through a browser using the OC://WebConnect Pro host and port only, not specifying another HTML file.

- **header.html** includes the OC://WebConnect Pro logo and version number and identifies the HTML page as the **Sessions** page.

- **sidebar.html** provides links to other OC://WebConnect Pro administration, configuration, and documentation functions.

- **footer.html** blends into the sidebar and contains the applet tag source when a session starts.

- **main.html** uses the **cgiinfo** utility and macros to provide the end user a list of session configurations. It also provides user options for applet type and SSL security and a **Start** button. Given the user choices when **Start** is chosen, **cgiinfo** queries the OC://WebConnect Pro server and produces the applet tag, which is returned to the browser combined with **tclient.html**.

- **tclient.html** is used as a template for the dynamic HTML that starts a session. The template includes a section in which the applet tag generated for the session is specified. If JavaScript is used for printing, JavaScript is included.

Caution

It is imperative to make a backup copy of the HTML files prior to any modification. It is recommended that the default HTML files be used for administrative and configuration purposes. The **cgiinfo.exe** uses the macros in these HTML templates to communicate with OC://WebConnect Pro to retrieve the requested information through a third-party HTTP server.

Examples of HTML Changes

Make a link to the OC://WebConnect Pro URL from a corporate Web page.

Example:

```
<P><A HREF="http://host1.oc.com:2080"><IMG SRC="hostaccess.gif" BORDER=0 HEIGHT=70
WIDTH=70></A></P>
```

Make the initial OC://WebConnect Pro HTML page a user page only (restrict administrative and configuration access).

Split the end user interface and the administrative interface; that is, remove end user access to the administrative and configuration options. Two simple ways to remove the administrative options are shown below:

- Replace the **index.html** file with the **main.html** file.
- Remove the **sidebar.html** frame from the **index.html** by deleting the following line from **index.html**:

  ```
  <FRAME NAME="Sidebar"
  SRC="sidebar.html?host=sultry.oc.com&port=4273&httpport=2081"
  SCROLLING=NO NORESIZE>
  ```

Change the look and feel of the Start Session page (index.html) to fit the existing corporate Web pages.

- Modify the **index.html**, **sidebar.html**, and **header.html** files to replace the OC://WebConnect Pro logos with corporate logos.
- Replace the background **.gif** file in **main.html** to match the background used by other pages on the corporate Web site.

Add or remove the end user configuration options when starting an emulation session.

Modify the **main.html** file to remove the list box for the applet type (**Ultra Lite**, **Enhanced,** and **Power User**), and add another input line to the **cgiinfo** call to hard code the applet type.

1. Delete the following lines:

```
<SELECT NAME="type">
<OPTION VALUE="lite">Hi mom
<OPTION VALUE="enhance">Enhanced
<OPTION VALUE="power">Power User
</SELECT>
<P>:
```

2. Add the following line below the other **cgiinfo** input type lines:

```
<INPUT TYPE="hidden" NAME="type" VALUE="lite">
```

Set up the user interface by department.

- Replace the **main.html** page with an HTML page that specifies departments or user groups.
- Similar to **main.html**, include links to new HTML pages that specify the correct OC://WebConnect Pro applet options for each department or group.
- Add password protection to the department or group pages that require additional security. For a simple logon implementation, see the **find.html** file in the OC://WebConnect Pro **samples** directory.

Use a CGI script to assign specific (“nail down”) 3287 LUs for printing.

A set of sample CGI scripts is provided with the OC://WebConnect Pro product for nailing down LUs to a specific user ID. See “CGI Scripts for Choosing LUs” for more information.

A copy of Perl must be installed on the platform where OC://WebConnect Pro is installed. **Winperl.exe** does not work on NT Platforms.

If you use a third-party Web server, it must reside on the same platform as OC://WebConnect Pro.

1. Copy the files listed below from **\wc\samples\3287resource** to the directories indicated:

    - **Find.html.** This is a sample HTML file that prompts the user for an ID and then initiates a CGI script. If you use a third-party Web server, place this file in the **/doc** directory of your HTTP server, If you use the OC://WebConnect Pro server, place this file in the **/wc/html** directory.
    - **Vg.pl.** This is a CGI script written in Perl. Place this file in the same directory as your CGI executable. If you use the OC://WebConnect Pro server and accepted the defaults at installation, the directory is **C:\WC**.

- **Vginfo.txt.** This is a flat file in which each line has a user ID with a host, port, and LU resource associated with it. If you use a third-party Web server, place this file in the **\doc** directory of your HTTP server, for example, in **\InetPub\wwwroot** if you use the Microsoft IIS Web server. If you use the OC://WebConnect Pro server, place this file in the **\wc\html** directory.

- **Vgtemplate.html.** This is a template used by **vg** to build a new HTML page. If you use a third-party Web server, place this file in the **\doc** directory of your HTTP server, for example, in **\InetPub\wwwroot** if you use the Microsoft IIS Web server. If you use the OC://WebConnect Pro server, place this file in the **\wc\html** directory.

2. Edit **vg.pl** and make the following changes if necessary. These four variables should be the only variables you change:

   - **#!/usr/local/bin/perl** – Change to the location of Perl and add the **.exe** extension to the Perl command.

   - **$filename = "/Netscape/Server/cgi-bin/ocs/vginfo.txt"**– Change to the location of the **vginfo.txt** file.

   - **$htmlfile = "/Netscape/Server/cgi-bin/ocs/vgtemplate.html"** – Change to the location of the **vgtemplate.html** file.

   - **$delimiter = "::"** – Change the delimiter to match the delimiter you use in your **.txt** file.

3. Edit the **vginfo.txt** file and modify the data as needed. The fields are user ID, host, port, and LU resource.

4. Establish a session and view the frame source with your browser. Copy the source and paste to a text document. Save the document as **\wc\html\vgtemplate.html**, which will overwrite the existing file.

   Note: If you do not want the user to see the button on the HTML page, change the applet values for height and width to 0.

Creating Static HTML to Download and Start an Emulation Applet

Applet tags with different parameters and parameter values are generated by OC://WebConnect Pro depending on the browser, browser version, and user choices of session configuration, applet type, and SSL. The macros and the **cgiinfo** interface to the OC://WebConnect Pro server provide dynamic applet tags based on the current server and session configurations, the browser used, and the user choices.

Not all applet tags work with all browsers, for example:

- An applet tag generated to work with a JDK 1.1 Java-enabled browser does not work with JDK 1.0 Java-enabled browsers.
- An applet tag generated when using Netscape or Internet Explorer might not work with HotJava.

Capturing the OC://WebConnect Pro Dynamic Applet Tag for Starting an Emulation Client

The applet tag source is generated when a session starts; the source does not exist until the **Start** button is chosen.

1. Start OC://WebConnect Pro and connect to the OC://WebConnect Pro **Start Sessions** page (**Index.html**).
2. Choose the session configuration, applet, and security settings.
3. Start a session. The applet appears and a connection is made.

   The HTML **Start Sessions** page, now showing on the browser, has four frames: **header**, **main**, **sidebar**, and **footer**. The applet tag is part of the **footer** frame in the lower part of the **Start Sessions** page.

5. Capture the applet tag source:

   Using Netscape, right-click the bottom left corner of the **Start Sessions** page and **View Frame Source**.

   -or-

   Using Internet Explorer, right-click the bottom of the **Start Sessions** page and select the pop-up menu option **View Source**.

6. Copy the HTML source code needed to a new HTML file.
7. Save the file in the HTML subdirectory in the directory containing the **wcd** OC://WebConnect Pro server.

The user can now access the new HTML file by including the HTML file name in the URL. Alternatively, a link to the new HTML file can be included on another HTML page.

Emulation Applet Tag parameters

To download and execute an applet, the browser needs to know what applet to download and where it is. The applet needs information and parameters to know what to do.

HTML instructs a browser to download and execute an applet and specifies the parameters for the applet. The HTML specific to a Java applet is called an *applet tag*. The applet tag is made up of the applet file names, the applet location on the HTTP server, and applet parameters.

Parameters for the OC://WebConnect Pro emulation applets include information such as the session configuration file name, SSL encryption and authentication information, and data overriding the session definition. More information on file names and applet parameters is provided below.

Applet Tag Syntax

<applet archive=*xxxxx.xxx* code=*xxxxx.class* CODEBASE="*/path*" width=*nnn* height=*nnn*>
<param name = "cabbase" value="*xxxx.cab*">
<param name ="*parametername*" value="*paramxxxx*">
</applet>

Applet File Name Information

Applet Tag	Description	Possible Values
<applet> </applet>	HTML keywords used as section delimiters specify applet information. All data between the <applet> and </applet> pertain to an applet.	None – just keywords that delimit the applet tag section.
archive	The file name of the Java applet package. A Java applet is a collection of Java class files. Applets are packaged differently depending on the browser and security option. Each browser supports a different format for packaging, compressing, and signing files. Internet Explorer does not use the archive setting.	See Table 1 – Applets Archive and cabbase Values for Applets Without SSL. -or- See Table 2 – Applets Archive and cabbase Values for Applets with SSL.
code	The class file to execute first. Each applet package (**.jar**, **.zip**, **.cab**) has many class files, so the one to run first must be specified. That class file calls and loads other class files as needed.	See Table 3 – Code Values.
CODEBASE	The subdirectory in which the Java applet files are located.	Default is /, relative to the OC://WebConnect Pro home

Applet Tag	Description	Possible Values
		directory and changes when a third-party HTTP server is used. If using a third-party HTTP server, specify this parameter as a full URL path to the location of the OC://WebConnect Pro emulation client packages.
width	The width of a button to display on the HTML page to allow the user to start another session. If autostart is set to 0, the button starts the first session.	Default is 0, meaning the button does not display.
height	The height of a button to display on the HTML page to allow the user to start another session. If autostart is set to 0, the button starts the first session.	Default is 0, meaning the button does not display.
MAYSCRIPT	Keyword that instructs the browser and applet that Java scripting can be accessed by the applet. Applies only to printing using the JavaScript solution.	Include keyword only if JavaScript is an option.
cabbase	The applet package for Internet Explorer to load. Other browsers ignore this option.	See Table 1 – Applets Archive and cabbase Values for Applets Without SSL. -or- See Table 2 – Applets Archive and cabbase Values for Applets with SSL.

Emulation Applet Parameters

Applet Parameter	Description	Possible Values
host	*Required parameter*. The host name or IP address of the platform where the OC://WebConnect Pro server runs. For security reasons, the Java 1.0 client software connects only to the server where the client originated, the machine that is the source of the download. This restriction is removed for signed Java 1.1 clients.	Any valid TCP/IP host name or IP address.
titlehost	The host name or IP to display in the title bar of the Java emulation applet.	Any valid TCP/IP host name or IP address.
port	*Required parameter*. The OC://WebConnect Pro Web server port established to listen for emulation traffic. If SSL is not being used, this is the Java or JCP port. If SSL is being used, this is the Java or Secure JCP port.	If a third-party server is specified, indicate the path to the emulation client Java and text files.
session	The file name of the session configuration file to use. This file name is determined when an administrator creates the session configuration file.	Default session file names: **def3270.ses** **def5250.ses** **def3287.ses** **defvt.ses** See the OC://WebConnect Pro **cfgdir/ses** directory for a list of all session file names.
Beepfile	The audio file to use for the emulation bell. The audio file plays when the host sends a bell character to the emulation client.	Default is **beep.au**. A different **.au** file can be used; it must be stored in the OC://WebConnect Pro **html** directory.
autostart	The number of sessions to automatically start.	Default is 1. Valid range is 0 to the license key limit minus 1. Specify 0 to load but not execute the applet. The end user can start the applet by clicking **Start Session**.
Button	A button to display to allow the user to start an initial session if autostart is set to 0. An additional session	Default is **Start Session**. The value for this option is the text string to display on the button.

Applet Parameter	Description	Possible Values
	starts if autostart is set greater than 0. To prevent an end user to start additional sessions, do not include this applet parameter.	
Htmlport	The port number set up to serve HTTP traffic. This could be the **wsd** port or a third-party server port. This option is required only for non-US English support of the **Ultra Lite** applets.	Default is 2080.
serverVersion	The version of the OC://WebConnect Pro emulation server to which the applet will connect. This version number is on the OC://WebConnect Pro status page and in OC://WebConnect Pro trace files.	WC plus the server version. Example: "WC3.2"
serverType	The platform type on which the OC://WebConnect Pro server is running.	UNIX or NT.
browserName	Required for running **Ultra Lite** applets.	MSIE, Netscape, or HotJava.
browserVersion	Required for running **Ultra Lite** applets.	The browser version number.
time	A time limit value for the Max session and client token authentication features.	This value must be generated by the OC://WebConnect Pro server.
Clickpad	Setting indicating whether to display the clickpad when the applet is initially displayed. The clickpad can be enabled or disabled via a client applet menu option.	ON or OFF.
emulation	The emulation type to use.	3270, 5250, VT, or 3287.
langname	The code for the client and/or emulation language. This language will be used for the client interface.	See Table 4 – Client Language Applet Tag Values.
Printimpl	The print solution to use for Print Screen and/or 3287 print.	none – Disable Print Screen and 3287 print functionality. JDKimpl – Use the JDK 1.1 print method embedded in the browser.

Applet Parameter	Description	Possible Values
		JSPrintImpl – Use JavaScript included in the HTML file and supported by the browser. JprintImpl – Use the OC://Webprint solution installed on the browser.
Maxsess	The maximum number of sessions that can be spawned from the applet’s **File**>**New menu** option.	0 – Disabled. 1 – Server license key maximum.
autofit	Option to allow the print solutions to automatically compress 132-column print onto a portrait page.	OFF or ON.
autogui	Option to enable the Auto GUI menu option on the Java emulation applet client. This option is valid only for **Power User** applets.	OFF or ON.
fontsize	Initial font size of host application text.	7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 20, or 24
script	TCL script file name. The file is stored in the **scripts** subdirectory, which is in the directory that contains the **wcd** OC://WebConnect Pro server. The file executes when the 3270 or 5250 Java client user enters **Ctrl+R** key combination at the keyboard.	Default is none. TCL scripts can have any valid file name with an extension of **.tcl**. They are stored in the OC://WebConnect Pro **scripts** directory followed by any script parameters. Space-delimit the file name and script parameters, for example: "sample1.tcl param1 param2"
Startup	TCL script file name that executes when the 3270 or 5250 Java client starts a new session. The script file is stored in the **scripts** subdirectory, which is in the directory that contains the b OC://WebConnect Pro server.	Default is none. TCL scripts can have any valid file name with an extension of **.tcl**. They are stored in the OC://WebConnect Pro **scripts** directory followed by any script parameters. Space-delimit the file name and script parameters, for example: "sample1.tcl param1 param2"
cipher	The cipher suite to be used for SSL authentication and encryption.	See Table 5 – SSL Cipher Suite Values.
certfpsv	SLL certificate generated by the OC://WebConnect Pro server.	Dynamically generated; cannot be used in static HTML.

Applet Parameter	Description	Possible Values
GatewayName	TCP/IP host name or IP address for the TN server or gateway to which the session should connect. This value overrides the session setting for host.	Any valid TCP/IP host name or IP address.
gatewayPort	The TCP/IP port on which the TN server or gateway listens for emulation traffic.	Default is 23.
GatewayResource	The TN server or gateway device name, such as an LU name or pool name.	Any valid LU name, device name, or pool name.

Applet and Applet Packages

Table 1 – Applet Archive and cabbase Values for Applets Without SSL

Netscape

Applets Without SSL	Netscape 3.x	Netscape 4.x
Ultra Lite		
3270, 5250, VT	Webconnect.zip	Webconnect.zip
3287	Webconnect3287.zip	Webconnect3287.zip
Enhanced		
3270	N/A	ns-E3270T.jar
5250	N/A	ns-E5250T.jar
VT	N/A	ns-EVTT.jar
3287	N/A	ns-E3287.jar
Power User		
3270, 5250,VT	N/A	ns-Emus.jar
3287	N/A	ns-E3287.jar
GUI Configurator	N/A	ns-Config.jar

Internet Explorer and HotJava

Applets without SSL	Internet Explorer 3.x	Internet Explorer 4.x	HotJava 1.x
Ultra Lite			
3270, 5250, VT	Webconnect.cab	Webconnect.cab	Webconnect.jar
3287	Webconnect3287.cab	Webconnect3287.cab	Webconnect3287.jar
Enhanced			
3270	N/A	E3270T.cab	E3270T.jar
5250	N/A	E5250T.cab	E5250T.jar
VT	N/A	EVTT.cab	EVTT.jar
3287	N/A	E3287.cab	E3287.jar
Power User			
3270, 5250, VT	N/A	Emus.cab	Emus.jar
3287	N/A	E3287.cab	E3287.jar
GUI Configurator	N/A	Config.cab	Config.jar

Table 2 – Applet Archive and cabbase Values for Applets with SSL

Netscape

Applets with SSL	Netscape 3.x	Netscape 4.x
Ultra Lite		
3270, 5250, VT	N/A	N/A
3287	N/A	N/A
Enhanced		
3270	N/A	ns-ssl-E3270T.jar
5250	N/A	ns-ssl-E5250T.jar
VT	N/A	ns-ssl-EVTT.jar
3287	N/A	ns-ssl-E3287.jar
Power User		
3270, 5250, VT	N/A	ns-ssl-Emus.jar
3287	N/A	ns-ssl-E3287.jar
GUI Configurator	N/A	ns-ssl-Config.jar

Internet Explorer and HotJava

Applets with SSL	Internet Explorer 3.x	Internet Explorer 4.x	HotJava 1.x
Ultra Lite			
3270, 5250, VT	N/A	N/A	N/A
3287	N/A	N/A	N/A
Enhanced			
3270	N/A	ssl-E3270T.cab	ssl-E3270T.jar
5250	N/A	ssl-E5250T.cab	ssl-E5250T.jar
VT	N/A	ssl-EVTT.cab	ssl-EVTT.jar
3287	N/A	ssl-E3287.cab	ssl-E3287.jar
Power User			
3270, 5250, VT	N/A	ssl-Emus.cab	ssl-Emus.jar
3287	N/A	ssl-E3287.cab	ssl-E3287.jar
GUI Configurator	N/A	ssl-Config.cab	ssl-Config.jar

Table 3 – Code Values

Applets	Netscape 3.x or Internet Explorer 3.x	Netscape 4.x, Internet Explorer 4.x, HotJava 1.x
Ultra Lite		
3270, 5250, VT	WebConnect.class	WebConnect.class
3287	WebConnect3287.class	WebConnect3287.class
Enhanced		
3270	N/A	COM.oc.webconnect.client.WebConnect3270Thin.class
5250	N/A	COM.oc.webconnect.client.WebConnect5250Thin.class
VT	N/A	COM.oc.webconnect.client.WebConnectVTThin.class
3287	N/A	COM.oc.webconnect.client.WebConnect3287Thin.class
Power User		
3270, 5250, VT	N/A	COM.oc.webconnect.client.WebConnectFat.class
3287	N/A	COM.oc.webconnect.client.WebConnect3287.class
GUI Configurator	N/A	COM.oc.webconnect.client.gui.config.ConfigFrame.class

Table 4 – Client Language Applet Tag Values

Client Language	HTML Applet Tag Value
Swiss German	de_CH
Swedish	sv_SE
German	de_DE
US English	en_US
British English	en_GB
Castilian Spanish	es_ES
French	fr_FR
Italian	it_IT
Japanese	ja_JP
Korean	ko_KR
Dutch	nl_NL
Norwegian	no_NO
Brazilian Portuguese	pt_BR
Turkish	tr_TR
Chinese Taiwan (traditional)	zh_tw
Chinese China (simplified)	zh_CN

Table 5 - SSL Cipher Suite Applet Tag Parameter Values

Cipher	Applet Tag Parameter Value
NULL	NULL or 0000
40-bit DES w/SHA-1 Message Authentication	0008
56-bit DES w/SHA-1 Message Authentication	0009
Triple DES w/SHA-1 Message Authentication	000A
40-bit RC4 w/MD5 Message Authentication	0003
128-bit RC4 w/MD5 Message Authentication	0004
128-bit RC4 w/SHA-1 Message Authentication	0005
MD5 Message Authentication (No Encryption)	0001
SHA-1 Message Authentication (No Encryption)	0002

Generating an OC://WebConnect Pro Applet Tag with CGI

The OC://WebConnect Pro CGI-BIN program **cgiinfo** can be used to retrieve HTML applet tag data from the OC://WebConnect Pro emulation server and start a session.

cgiinfo provides all the applet parameters necessary to match the HTML applet tag data to the browser and browser version with the latest configuration data collected from the end user and OC://WebConnect Pro HTML files. The use of **cgiinfo** is required for using the OC://WebConnect Pro implementation of SSL and client token authorization.

The CGI-BIN parameters passed from the HTML, through the CGI-BIN, to OC://WebConnect Pro use a **name=value** format. Following is a list of possible parameters passed from HTML templates to the CGI-BIN for communication with OC://WebConnect Pro to retrieve requested information.

HTML Macros Passed to cgiinfo

To dynamically create HTML that includes up-to-date applet parameters, OC://WebConnect Pro provides a CGI-BIN interface called **cgiinfo**. **cgiinfo** allows an HTTP server to query the OC://WebConnect Pro emulation server for the latest configuration information. With this information, the applet tag portion of the HTML is generated dynamically.

The macros and parameters are passed to the OC://WebConnect Pro emulation server through the administration port. **cgiinfo** is used by the default **Index.html** and other HTML templates to retrieve information to construct an applet tag for an HTTP server. The HTTP server can be the OC://WebConnect Pro HTTP server **wsd** or a third-party server.

The input parameters to **cgiinfo** are listed below:

- Data required to contact the OC://WebConnect Pro emulation server
- Specific session file to use to generate the applet tag
- Options not set in the session file
- Information for producing the necessary HTML data

Html Example of cgiinfo Use

<FORM ACTION="*/cgi/cgiinfo*" METHOD=POST TARGET="*xxxxx*">
<INPUT TYPE="*hidden*" NAME="*parameter namet*" VALUE="*xxxx*">
</FORM>

Input Parameters for cgiinfo

Parameter	Description	Values
hostname	The host name where OC://WebConnect Pro emulation server **wcd** is running.	Any valid domain name server host name or TCP/IP address.
portnum	The administration port for OC://WebConnect Pro emulation server.	Any valid TCP port number. Default is 4270.
command	The request command.	**Start** – Start a session.
type	The session type to use.	**Ultra Lite**, **Enhanced**, or **Power User**.
ssl	Indicator of whether or not to use Secure Socket Layer (SSL) protocol.	ON or OFF
count	The number of sessions to start when the applet is loaded.	1 – Default. 0 – No sessions will autostart.
sfile	The session file to use. The session file should correspond to the emulation **type**.	Example: **def3270.ses** Valid file names are any **.ses** files stored in the OC://WebConnect Pro **cfgdir/ses** directory.
http	The HTTP port to use for **Ultra Lite** sessions.	Any valid TCP port.
mode	The operation mode.	**Cooked** means perform HTML macro expansion.
HTMLfile	The HTML file name to use for macro substitution. The path to this file should be relative to the home directory of the **cgiinfo** process. The default is **tclient.html**. See the **tclient.html** file for an example or to modify the existing **tclient.html** file. The **cgiinfo** process inserts the applet tag data into the area of the HTML file specified for applet tag macro substitution by the string **|applpara|**. The combined HTML code is then sent to the browser to start an applet. The file can contain any valid HTML commands, but must include the macro substitution section.	Any valid HTML file stored on the same system as the **cgiinfo** process. Should have the following section for macro substitution: <!----macro begin------> |applpara| <!----macro begin----- >

Parameter	Description	Values
Print	The chosen print implementation.	**JDK** – Use the JDK1.1 print solution. **JS** – Use the JavaScript print solution. **OCWP** – Use the OC://WebPrint solution. **None** – Use no print solution and disable client print options. **Default** – Use the default print solution specified in the session file.
outfile	The file name to use for output.	Optional. Any valid file name.

Example HTML Code Using cgiinfo

```
<!-- WebConnect Pro HTML -->
<HTML>
<HEAD>
<TITLE>OC://WebConnect Pro - Sessions</TITLE>
</HEAD>
<BODY BACKGROUND="/images/whiteroc.gif" LINK="#281860" VLINK="#281860">
<FORM ACTION="/cgi/cgiinfo" METHOD=POST TARGET="Footer">
<INPUT TYPE="hidden" NAME="cmd" VALUE="start">
<INPUT TYPE="hidden" NAME="host" VALUE="host1.oc.com">
<INPUT TYPE="hidden" NAME="type" VALUE="lite">
<INPUT TYPE="hidden" NAME="sfile" VALUE="def3270">
<INPUT TYPE="hidden" NAME="port" VALUE="4270">
<INPUT TYPE="hidden" NAME="mode" VALUE="cooked">
<INPUT TYPE="hidden" NAME="html" VALUE="html/tclient.html">
<INPUT TYPE="hidden" NAME="http" VALUE="2080">
<INPUT TYPE="hidden" NAME="count" VALUE="1">
</FORM>
</BODY>
</HTML>
```

Output from cgiinfo

cgiinfo writes the HTML with the file name specified in the **cgiinfo html** parameter and the applet tag generated. The applet tag is inserted in the original HTML file in the **applpara** section. The **applpara** should be specified as follows:

```
<!---macro begin---------->
|applpara|
<!---macro end------------>
```

☞

> **Note:** If you use the **Ultra Lite** applet, OC://WebConnect Pro and the HTTP Web server must reside on the same machine.

Working with a Third-Party HTTP Server

The OC://WebConnect Pro HTTP server functionality can be provided by a third-party HTTP server. The ability for a third party to process HTML pages for an end user and deliver a Java emulation session can be accomplished fairly easily. Once the Java emulation session is downloaded, the HTTP server is no longer used. A direct persistent connection is used for the emulation traffic between the emulation clients and the OC://WebConnect Pro emulation server.

There are two general ways that OC://WebConnect Pro can work with a third-party HTTP server:

- The third-party server can use the OC://WebConnect Pro **cgiinfo** to communicate with the OC://WebConnect Pro server to obtain the latest configuration data and dynamic applet tags.
- Static HTML with static applet tags can be written and maintained to download the emulation client applets to the browser.

Many third-party HTTP Web servers work differently from others. This section contains general instructions for working with third-party HTTP Web servers.

Using Static HTML Code

Most commercial Web servers provide a configuration utility that allows alternate document directories to be configured.

1. Use the Web server configuration utility to create an alternate document directory such as **/wc**. Point that alternate directory to the OC://WebConnect Pro **html** directory (default is **/wc/html**). When this is configured correctly, the third-party Web server can access the OC://WebConnect Pro HTML directory with this URL:

   http://host1.oc.com/wc

2. Modify the **CODEBASE** and **htmlport** values specified in the applet tag section of the HTML file used to start applets to the host name plus the third-party server **/wc** directory. Example:

   ```
   <applet CODEBASE=http://host1.oc.com/wc archive-WebConnect.zip code=WebConnect.class.
   width=150 height=25>
   <param name=htmlport value=/wc>
   ```

It might be necessary to move the Java emulation client files to the third-party HTTP server directory.

Ultra Lite applets require the third-party server to be on the same machine as the OC://WebConnect Pro emulation server. This limitation is based on the security model provided with JDK 1.0 Java-enabled browsers.

A text file called **wcJStrings.txt** provides the text for the applet menus and dialogs. This file is available for each client language supported.

Note: To use **Ultra Lite** applets, copy **wcJStrings.txt** to the third-party directory from the OC://WebConnect Pro **NLS** directory under a specific language directory.

Customizing the Client Interface

The ability to customize the emulation client applet interface can often be accomplished by choosing the right applet type. If the need to customize the applet is greater, OpenVista provides the ability to make extensive changes and even replace the applet user interface.

Some of the need to customize the emulation client applet interface is solved with the availability of the different applet types and individual features like **Auto GUI**. **Ultra Lite** applets are available for the low-end user, **Enhanced** applets are available for the user who needs more functionality, and **Power User** applets are for those users who need file transfer and **Auto GUI** functionality.

OpenVista is a Java Integrated Development Environment with both visual and simple API access to the OC://WebConnect Pro Java emulation applets. OpenVista provides both the ability to make minor changes to many user interface features of the standard applets and, more importantly, provides the capability to develop a completely different and custom emulation interface. This capability allows the development of new Java applets using OC://WebConnect Pro Java code to provide the emulation engine and connectivity to the OC://WebConnect Pro server.

More Information

- For more information about the different emulation client applet types, see *Chapter 11: Emulation Client Applet Interface and Features*.
- For more information about OpenVista, see the *OpenVista User’s Guide* provided online with OpenVista.

Chapter 13: TCL Scripting Extensions

Customizing Client Access to Host Applications

OC://WebConnect Pro incorporates the TCL embeddable scripting language from Sun Microsystems. Using the standard TCL scripting language along with several extensions provided with OC://WebConnect Pro, you can customize client access to 3270 and 5250 host applications.

Arguments can be passed to the TCL script by supplying the arguments, following the script name as part of the applet parameters, for example:

```
<param name="script" value="script.tcl arg1 arg2 arg3">
```

beep(3WC) Extension

Name

beep - play the **beep** audio file.

Synopsis

beep

Description

beep instructs the 3270 Java client software to play the default “beep” file. The default “beep” file is specified in the HTML file which downloads the 3270 Java Applet.

The audio file, **beep.au** is located in the **html** subdirectory of the directory where the OC://WebConnect Pro server resides in the default **beep** file.

Return Value

On successful completion, **beep** returns **R_OKAY**. Otherwise, an error is returned which passes to **query error message** for more information.

Errors

On failure, **beep** returns the following error:

[ENOFILE] The default **beep** file does not exist.

Example

```
set errno [beep]
if { $errno != "R_OKAY" } {
puts "\"beep\" failed, [query error message $errno]"
exit 1
}
```

copy(3WC) Extension

Name

copy - copy data to/from the screen buffer.

Synopsis

copy to [*session ID*] [position] *position* [text] *string*

copy from [*session ID*] [position] *position* [length] *length*

Description

copy copies data to or from the screen buffer.

ID specifies the session ID of a host session. If session *ID* is omitted, copy copies data to or from the screen buffer associated with the default session. Set the default session ID with the default command.

position specifies the screen position where the data is copied to or from. Specify position as an offset into the screen buffer or by row and column as follows:

> **row** *row* **column** *column*

The **row** and **column** keywords are required if the *position* is specified by row and column instead of screen buffer offset value.

string specifies the data to be copied to the screen buffer.

length specifies the maximum length of the data copied from the screen buffer.

Return Value

On successful completion, **copy** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

In addition, **copy** from returns the length of the returned data, followed by the requested data. The **TCL** list returned by **copy from** has the following format:

Element #	Description
0	the return code.
1	the length of the requested data.
2	the requested data.

Retrieve the elements of the returned list individually with the **lindex** command.

Errors

On failure, copy returns one of the following errors:

[EINVALID]	The specified *position* is invalid.
[ENOSESSION]	The specified session *ID* or the default session ID is invalid.

Example

```
set data [copy from position 234 length 15]
set errno [lindex $data 0]
if { $errno != "R_OKAY" } {
puts "\"copy from\" failed, [query error message $errno]"
exit 1
}
puts "[lindex $data 1] bytes successfully copied ..."
puts "[lindex $data 2]"
```

default(3WC) Extension

Name

default - set OC://WebConnect Pro defaults.

Synopsis

default [*parameter* [=] *value*] [...]

Description

default allows you to change OC://WebConnect Pro defaults.

parameter specifies the OC://WebConnect Pro parameter to change. User-modifiable parameters are described in the following table:

Parameter	Value	Description
keyboard	**locked** **unlocked**	lock the 3270 Java client's keyboard unlock the 3270 Java client's keyboard
session	*ID*	default session ID
timeout	*minutes* **minute[s]** *seconds* **second[s]**	default **wait** timeout specified in minutes and seconds

If *parameter* is omitted, **default** returns a list of user modifiable parameters along with the current value of each parameter.

Return Value

On successful completion, **default** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

In addition, **default** returns a list of parameter/value lists containing the previous value of each parameter which was modified. If no parameters were modified, the name and current value of all user modifiable parameters returns.

Each *parameter*/*value* list contains the following elements:

Element #	Description
0	parameter name.
1	parameter value.

The individual parameters return values as follows:

Parameter	Value
keyboard	**locked or unlocked**
session	The session ID.
Timeout	The timeout value in seconds

Retrieve the elements of the returned list individually with the **lindex** command.

Errors

On failure, default returns one of the following error:

[EINVALID] An invalid parameter was specified.

Example

```
set data [default timeout 1 minute 30 seconds keyboard locked]
set errno [lindex $data 0]
if { $errno != "R_OKAY" } {
        puts "\"default\" failed, [query error message $errno]"
        exit 1
}
set value [lindex $data 1]
puts "The previous timeout was [lindex $value 1] seconds."
set value [lindex $data 2]
puts "The keyboard was [lindex $value 1]."
```

move(3WC) Extension

Name

move - moves the cursor to a new position.

Synopsis

move [**cursor**] [**to**] [session *ID*] [position] *position*

Description

move moves the cursor to the specified position.

ID specifies the session ID of a host session. If **session** *ID* is omitted, **move** moves the cursor associated with the default session. The default session ID may be set with the **default** command.

position specifies to which the screen position to move the cursor. Specify *position* as an offset into the screen buffer or by row and column as follows:

row *row* **column** *column*

The **row** and **column** keywords are required if the position is specified by row and column.

Return Value

On successful completion, **move** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

Errors

On failure, move returns one of the following errors:

[EINVALID]	The specified position is invalid.
[ENOSESSION]	The specified session ID or the default session ID is invalid.

Example

```
set result [move cursor to row 10 column 12]
if { $result != "R_OKAY" } {
        puts "\"move\" failed, [query error message $result]"
        exit 1
}
```

query(3WC) Extension

Name

query - return requested information

Synopsis

query cursor [*position*] [*session ID*]

query error [*message*] *errno*

query field [*session ID*] [[*position*] *position* [*modifier*]]

Description

query returns the requested information.

query cursor returns the current cursor position.

session ID specifies the session ID of a host session. If *session ID* is omitted, **query cursor** returns the current cursor position of the default session. The default session ID can be set with the **default** command.

query error returns a descriptive error message for the error specified by *errno*. *errno* may be specified as a numerical value or as a mnemonic which was returned by another OC://WebConnect Pro TCL extension.

query field returns information about a specific field.

session ID specifies the session ID of a host session. If *session ID* is omitted, **query field** returns information for fields associated with the default session. The default session ID can be set with the **default** command.

position specifies the screen position of interest. *position* can be specified as an offset into the screen buffer or by row and column as follows:

row *row* **column** *column*

the **row** and **column** keywords are required if the *position* is specified by row and column. If *position* is omitted, field information is returned for all fields on the current screen.

modifier specifies the field for which the information is to be returned. *modifier* may be any one of the following:

this field
previous field
next field
next protected field
next unprotected field
previous protected field
previous unprotected field

If *modifier* is omitted, field information is returned for "this field" (the field including the screen position specified by *position*).

Return Value

On successful completion, **query** returns **R_OKAY**. Otherwise, an error is returned which can be passed to **query error message** for more information.

> **Note: query error** returns a descriptive error message for the specified error. No other values are returned. In addition, **query** returns the requested information.

The TCL list returned by query has the following format:

Element #	Description
0	the return code.
1	the requested information.

The requested information is returned in various formats depending on the information returned.

query cursor returns the current cursor position as an offset into the screen buffer.

query field returns a TCL list containing the field information for the specified field(s). If *position* is omitted, a field information list is returned for each field on the current screen.

Each field information list contains the following elements:

Element #	Description	Values
0	Field Position	*position*
1	Field Length	*length*
2	Field Type	**Protected** **Unprotected**
3	Data Type	**Numeric** **Alphanumeric**
4	Display Mode	**Normal intensity, pen not detectable** **Normal intensity, pen detectable** **High intensity, pen detectable** **Non-display, pen not detectable**
5	Field Status	**Modified** **NOT modified**

The elements of the returned list can be retrieved individually with the **lindex** command.

Errors

On failure, query returns one of the following errors:

[EINVALID] An invalid keyword was specified.

[ENOSESSION] The specified session ID or the default session ID is invalid.

Example

```
set data [query cursor position]
set errno [lindex $result 0]
if { $errno != "R_OKAY" } {
        puts "\"query\" failed, [query error message $errno]"
        exit 1
}
puts "Current Cursor Position: [lindex $data 1]"
```

search(3WC) Extension

Name

search - searches the screen buffer for specific data.

Synopsis

search [d*irection*] [**for**] [**text**] *string* [**from**] [*session ID*]

[[**position**] *position*]

Description

search searches the screen buffer for specific data.

direction specifies the direction in which the search is to proceed. *direction* must be one of the following:

forward
backward
all

If *direction* is omitted, **search** searches forward from the specified position.

string specifies the text string to be searched for.

session ID specifies the session ID of a host session. If *session ID* is omitted, **search** searches the screen buffer associated with the default session. Set the default session ID with the **default** command.

position specifies the screen position where the search begins. Specify *position* as an offset into the screen buffer or by row and column as follows:

row *row* **column** *column*

The **row** and **column** keywords are required if the *position* is specified by row and column. If *position* is omitted, the search starts at the beginning of the screen buffer (the default position is **1**).

Return Value

On successful completion, **search** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

In addition, **search** returns the screen position where *string* is found. The **TCL** list returned by **search** has the following format:

Element #	Description
0	the return code.
1	the screen position where *string* is found

Retrieve the elements of the returned list individually with the **lindex** command.

Errors

On failure, search returns one of the following errors:

[ENOTFOUND] The specified string was not found in the screen buffer, or was not found at the location specified by position.

[ENOSESSION] The specified session ID or the default session ID is invalid.

Example

```
set data [search forward for text "Hello, world!" from position 0]
set errno [lindex $data 0]
if { $errno != "R_OKAY" } {
   puts "\"search\" failed, [query error message $errno]"
   exit 1
}
puts "Text string found at screen position [lindex $data 1]"
```

sendfile(3WC) Extension

Name

sendfile - sends files to the 3270 Java client.

Synopsis

sendfile [[**audio**] [file] *audio_file*]

Description

sendfile sends files to the 3270 Java client.

audio_file is the name of an audio file sent to the 3270 Java client. The file plays immediately upon receipt. If the file name ends with the extension **au**, the keyword **audio** can be omitted.

Multiple files can be sent to the 3270 Java client with one **sendfile** command.

Return Value

On successful completion, **sendfile** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

Errors

On failure, **sendfile** returns one of the following errors:

[ENOFILE]	The specified file does not exist.

Example

```
set errno [sendfile audio beep.au]
if { $errno != "R_OKAY" } {
        puts "\"sendfile\" failed, [query error message $errno]"
        exit 1
}
```

sendkey(3WC) Extension

Name

sendkey - sends function keys, data, and/or an AID key to the host.

Synopsis

sendkey [*session ID*] [**key** *key_code*] [[**text**] *string*] [**aidkey** *AID_Key*]

Description

sendkey sends keystrokes, including attention identifier (AID) keys, to the host.

session ID specifies the session ID of a host session. If *session ID* is omitted, sendkey sends the specified keystrokes to the host using the default session ID. Set the default session ID with the **default** command.

key_code specifies one or more of the key codes described in the following tables:

3270 Key Codes
5250 Key Codes

string specifies ASCII data to be sent to the host. ASCII mnemonics, representing special function keys described in the tables below, can be embedded directly in a text string. Otherwise, key codes must be preceded by the **key** keyword.

Multiple key codes and text may be interspersed on one **sendkey** command line.

AID_Key specifies one of the 3270 or 5250 AID keys described in the following tables:

3270 AID Keys
5250 AID Keys

> **Note:** Only one AID key can be specified on a **sendkey** command line. Everything after the first AID key is discarded. This restriction may be removed in the future.

Return Value

On successful completion, **sendkey** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

Errors

On failure, **sendkey** returns one of the following errors:

[ETRUNCATED] Output was terminated after the first AID key, and all following data was truncated.

[ENOSESSION] The specified session ID or the default session ID is invalid.

Example

```
set result [sendkey "Hello, world!" aidkey Enter]
if { $result != "R_OKAY" } {
puts "\"sendkey\" failed, [query error message $result]"
exit 1
}
```

3270 Attention Identifier (AID) Keys

Control Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
Attn	@A@Q	System Request	@A@H	PA1	@x
Clear	@C	.	.	PA2	@y
Enter	@E	.	.	PA3	@z

Programmable Function Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
PF1	@1	PF7	@7	PF13	@d	PF19	@j
PF2	@2	PF8	@8	PF14	@e	PF20	@k
PF3	@3	PF9	@9	PF15	@f	PF21	@l
PF4	@4	PF10	@a	PF16	@g	PF22	@m
PF5	@5	PF11	@b	PF17	@h	PF23	@n
PF6	@6	PF12	@c	PF18	@i	PF24	@o

5250 Attention Identifier (AID) Keys

Control Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
Clear	@C	Help	@H	RollUp	.
Enter	@E	Print	@P	RollDown	.

Function Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
F1	@1	F7	@7	F13	@d	F19	@j
F2	@2	F8	@8	F14	@e	F20	@k
F3	@3	F9	@9	F15	@f	F21	@l
F4	@4	F10	@a	F16	@g	F22	@m
F5	@5	F11	@b	F17	@h	F23	@n
F6	@6	F12	@c	F18	@i	F24	@o

3270 Key Codes

Control Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
CursorSelect	@A@J	EraseEOF	@F	Print	@P
FieldMark	@S@y	EraseInput	@A@F	Reset	@R

Cursor Movement Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
CursorUp	@U	NewLine	@N	Home	@0
CursorDown	@V	Tab	@T	WordLeft	@A@z
CursorLeft	@L	Backtab	@B	WordRight	@A@y
CursorRight	@Z	.	.	.	.

Cursor Attribute Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
AlternateCursor	@$	CursorGr?	.

Edit Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
Backspace	@<	Delete	@D	Insert	@I
Dup	@S@x	DeleteWord	@A@D	.	.

Text Attribute Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
HighDefault	.	HighUnderscore	.
HighReverse	.	HighBlink	.

Text Color Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
Red	@A@d	Yellow	@A@g	White	@A@j
Pink	@A@e	Blue	@A@h	ResetHostColors	@A@l
Green	@A@f	Turquoise	@A@i	.	.

5250 Key Codes

Control Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
Attention	@A@Q	SystemRequest	@A@H
Reset	@R	Test	@A@C

Cursor Movement Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
CursorUp	@U	Return	@N	Home	@0
CursorDown	@V	Tab	@T	DoubleLeft	.
CursorLeft	@L	Backtab	@B	DoubleRight	.
CursorRight	@Z	.	.	.	.

Field Navigation Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
FieldPlus	@A@+	FieldMinus	@A@-	FieldExit	@A@E

Edit Keys

Key Code	ASCII Mnemonic	Key Code	ASCII Mnemonic
Backspace	@<	Delete	@D
Dup	@S@x	Insert	@I

Text Assist Keys

Key Code	Command Description	Key Code	Command Description
AltA	Insert Symbols	AltUp	Top of Page
AltB	Begin Bold	AltDown	Bottom of Page
AltC	Center Text	AltLeft	Beginning of Line
AltD	Next Text Column	AltRight	End of Line
AltH	Half Index Down	AltFieldPlus	Carrier Return
AltJ	End Bold/Underscore	AltFieldMinus	Carrier Return
AltN	Stop Code Advance	AltFieldExit	Carrier Return
AltP	Page End	AltSpace	Required Space
AltS	Stop Code Function	AltTab	Required Tab
AltU	Begin Underscore	AltBacktab	Shifted Tab
AltW	Word Underscore	.	.
AltY	Half Index Up	.	.

wait(3WC) Extension

Name

wait - suspends the TCL script.

Synopsis

wait [*timeout*] [**for**] **keyboard** [**unlock**] [*session ID*]

wait [*timeout*] [**for**] **screen** [**update**] [*session ID*]

wait [*timeout*] [**for**] [**text**] *string* [**at**] [*screen ID*]

[[**position**] *position*]

Description

wait suspends the TCL script until the specified event occurs. If the specified event has already occurred, **wait** returns immediately.

wait for keyboard returns when the host unlocks the keyboard after receiving an AID key.

wait for screen returns when the screen buffer is updated by the host.

wait for *string* returns when *string* is found at the specified position in the screen buffer. If position is omitted, **wait** returns when *string* is found anywhere in the screen buffer.

timeout specifies a length of time after which **wait** returns regardless of whether or not the specified event has occurred. If the specified event does not occur within the specified time, wait returns to the caller with an appropriate return code. Specify *timeout* as follows:

[**timeout**] *minutes* **minute[s]** *seconds* **second[s]**

string specifies the text string for which you are searching.

session *ID* specifies the session ID of a host session. If **session** *ID* is omitted, **wait** waits for the specified event to occur for the default session. Set the default session ID with the **default** command.

position specifies the screen position (for example, wait returns when *string* appears at the specified screen position or when the command times out.) Specify *position* as an offset into the screen buffer or by row and column as follows:

row *row* **column** *column*

The **row** and **column** keywords are required if the position is specified by row and column.

Return Value

On successful completion, **wait** returns **R_OKAY**. Otherwise, an error returns that passes to **query error message** for more information.

In addition, **wait** returns an offset into the screen buffer where the specified data begins. If no data was specified, an offset of **0** is returned. The **TCL** list returned by **wait** has the following format:

Code	Description
0	Return code
1	Offset into the screen buffer where *string* begins

Retrieve the elements of the returned list individually with the **lindex** command.

Errors

On failure, **wait** returns one of the following error:

[ETIMEDOUT] The specified timeout period elapsed before the waited for event occurred.

[ENOSESSION] The specified session ID or the default session ID is invalid.

Example

```
set data \
    [wait 1 minute 15 seconds for text "Hello, world!" at position
100]
set errno [lindex $data 0]
if { $errno == "ETIMEDOUT" } {
     puts "\"wait\" timed out!"
     exit 0
}
if { $errno != "R_OKAY" } {
     puts "\"wait\" failed, [query error message $errno]"
     exit 1
}
set offset [lindex $data 1]
puts "Text string found at screen position $offset."
```

Chapter 14: Transferring Data Files

Using IND$FILE Transfer

OC://WebConnect Pro transfers files between a Java client and an SNA host application using the standard IND$FILE transfer protocol. A variety of networking needs including centralized data backups and data warehousing through an SNA host may make use of this functionality.
Because SNA host files use different file formats than OC://WebConnect Pro 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.

The following table lists the SNA hosts and SNA applications used for transferring files (including the IBM program number and operating system for each application).

Application Program	Program Number	Operating system
3270 PC File Transfer for CICS/VS	5798-DQH	VS
3270 PC File Transfer for TSO	5665-311	MVS
3270 PC File Transfer for VM/CMS	5664-281	VM

☞

Notes

- OC://WebConnect Pro supports only the DFT (Distributed Function Terminal) file transfer mode.
- IND$FILE transfer is available only when using the OC://WebConnect Pro **Power User** Java applet.
- You must be familiar with the file transfer application program you want to use.

Sending and Receiving CICS/VS Files

OC://WebConnect Pro enables file transfer between a Java client and the Customer Information Control System/Virtual Storage (CICS/VS) SNA application. You can use the Java client's **Transfers** menu for transferring files to suit your needs.

To transfer files to and from CICS/VS, use the following steps:

1. Make sure the Java client is connected to a desired SNA host and CICS application.
2. Select **File Transfer** from the **File** Menu.
3. Select **IND$FILE** from the **File Transfer** menu.
4. Select either **Send to Host** or **Receive from Host** from the **IND$FILE** submenu.
5. Select the **CICS** option. The appropriate file transfer window displays with the hostname of the active session.
6. Click the **Local File** button to search for the peer's file. A file selection window displays. The procedures for searching for the peer file name vary with your system. After you select the peer file, the name displays in the text field to the right of the **Local File** button.
7. Click the **UNIX Format** button if you want to transfer files in UNIX format. This allows line separators to be converted to carriage return and line feed pairs during a Send operation. During a Receive operation, carriage return and line feed pairs are converted to line separators.
8. Type a host file name in the **CICS File Name** field in the **File Attributes** box.

☞

> **Note:** The CICS file name can be a program name, a transaction identification, or identification selected by the CICS/VS application programmer. If the file name does not exist, the CICS/VS application automatically creates it. The file name can be entered as 1–8 characters in length. The character in position 1 must be entered as a letter; characters in positions 2–8 can be entered as letters or digits.

9. Type comments about the file being transferred in the **Comments** field in the **File Attributes** box. The comments are automatically installed in the first record of the CICS/VS host file.

10. Select a file type from the **Transfer Options** box to configure the way the file’s contents are treated during the transfer process. The choices are described below:

ASCII	This option instructs the SNA host to translate data between the EBCDIC and ASCII character formats. You can use this option for translating ASCII formatted files, such as text edit files or print files. You should not use the ASCII option for transferring binary data (such as output data from a database program) or object code files (such as C compiler object code).
Binary	This option instructs the SNA host to perform no character translation. The option can be used to transfer encrypted data, compiled programs, and other data that is unreadable.

Caution

Do not click the **UNIX Format** check box when activating the **Binary** option or the binary data becomes corrupted.

Notes

- If you do not specify the **CRLF** option in the Send mode, the SNA host disregards the local file’s line separators.
- You should not use the CRLF option for transferring binary data (such as output data from a database program) or object code files (such as C compiler object code)
- You can click the **UNIX Format** check box for ASCII file transfers. This allows line separators to be converted to carriage return and line feed pairs during a Send operation. During a Receive operation, carriage return and line feed pairs are converted to line separators.
- Invoking the **No CRLF** option in the Receive dialog box instructs the CICS/VS host to copy the file unaltered to the appropriate TCP/IP host. The **No CRLF** option can be used to transfer encrypted data, compiled programs, and other data that is unreadable.

12. Select **CRLF** or **No CRLF**.

13. Click the **Cancel** button to disregard your settings.

    -or-

    Click the **OK** button to begin file transfer.

Sending and Receiving TSO Files

The features of OC://WebConnect Pro features allow you to transfer files between a Java client and the Time Sharing Option (TSO) SNA application. You can use the Java client’s **Transfers** menu for transferring files to suit your needs.

To transfer files between your directory system and a TSO application, follow these steps:

1. Make sure the Java client is connected to a desired SNA host and TSO application.
2. Select **File Transfer** from the **File** menu.
3. Select **INDFile** from the **File Transfer** menu.
4. Select either **Send to Host** or **Receive from Host** from the **INDFile** submenu.
5. Select the **TSO** option.
6. Click the **Local File** button to search for the peer’s file. A file selection window displays. The procedures for searching for the peer file name vary with your system. After you select the peer file, the name displays in the text field to the right of the **Local File** button.
7. Click the **UNIX Format** button if you want to transfer files in UNIX format. This allows line separators to be converted to carriage return and line feed pairs during a Send operation. During a Receive operation, carriage return and line feed pairs are converted to line separators.
8. Type a data set name in the **TSO Data Set Name** field.
9. Type a member name in the **Member Name** field.

☞

Notes

- The TSO host data set name must conform to IBM naming conventions. You can enter an existing data set name (stored in your library) or a new data set name.
- No closing quote displays in the **Member Name** field.

Notes

- The member name is optional. If entered, the member name should be a member in a partitioned data set directory.
- When you use the **Send** dialog box to copy a file to a partitioned data set and include a member name, the partitioned data set must exist. OC://WebConnect Pro does not create the partitioned data set.
- The TSO application adds a user ID prefix to the combined data set and member name. To eliminate the user ID prefix, enclose the data set and member name in single right quotation marks, such as ’smith.pds2.file1’.

10. Type the appropriate password in the **Password** field. A password is required only if password-protection has been specified for the TSO data set.

11. Select a transfer option from the **General** box in the **Transfer Options** area. The **Transfer Options** parameters allow you to configure the way the file’s contents are treated during the transfer process. The choices are described below:

Append	This option allows you to append a local file to the end of an SNA host file; otherwise, you can append an SNA host file to a local file. The Append option overrides any other values specified by the LRECL parameter and RECFM options.
ASCII	This option instructs the SNA host to translate data between the EBCDIC and ASCII character formats. You can use this option for translating ASCII formatted files, such as text edit files or print files.
CRLF	This option (by using the Send dialog) instructs the SNA host to replace the local file line separators with SNA record separators. If you use the Receive dialog, the SNA host replaces the SNA record separators with local file line separators. If you do not specify the CRLF option in the Send mode, the SNA host disregards the local file’s line separators.

Note: When you send a file to a TSO application, the local file’s line separators are replaced with record separators. When a Java client receives a file, the SNA host record separators are replaced with line separators. If you do not specify the CRLF option in the Send mode, the SNA host disregards the local file’s line separators.

Caution

Do not use the ASCII or CRLF options for binary data (such as output data from a data base program) or object code files (such as C compiler object code).

12. Select a record format parameter for the SNA host file from the **Format** box in the **Transfer Options** area. The **Format** check boxes specify the record format of the SNA host file. This is only valid if you are sending a file. Values are:

Fixed	Indicates that the data set’s records are fixed length
Variable	Indicates that the data set’s records are variable length
Undefined	Indicates that the data set contains undefined record lengths
None	Indicates no record format is to be used

13. Select the **Specify Space Parameters** check box in the **Allocation Units** area to set the amount of space to be allocated for a new data set. The **Blocks**, **Tracks**, and **Cylinders** radio buttons are enabled. If the Space toggle button is not activated, the TSO application uses the Blocks parameter’s default value. This is only valid if you are sending a file. Values are:

Blocks	This parameter represents the smallest storage entity to be used.
Tracks	This parameter represents the middle-sized storage entity to be used.
Cylinders	This parameter represents the largest storage entity to be used.
Primary	This parameter lets you specify the primary allocation for the **Blocks** parameter.
Increment	This parameter lets you specify the increment allocation for the Blocks parameter.

14. Type a size value in the **BLKSIZE** field in the **Transfer Options** area. You can enter the data block size of a TSO data set. The variable you enter represents a data block’s number of bytes. The default value is 80. This is only valid if you are sending a file.

Notes

You might be replacing a file or appending one file to another file. If so, the TSO application uses the existing file’s block size information—the BLKSIZE parameter is not used. In addition, the TSO application uses the file transfer operation’s default record length if the BLKSIZE parameter is not activated.

15. Type a logical record length value of the SNA host file in the **LRECL** field in the **Transfer Options** area. The parameter value represents the number of characters for each record. If the parameter is not entered, the record length is determined by the file transfer operation. For new files, the parameter's default value is 80.

    If you are replacing a file or appending information to a file, the characteristics of the existing file are used. If you are transferring variable length records, the parameter represents the maximum record size. If you do not send a record of the maximum operating system size, the parameter's value becomes the longest record sent. This is only valid if you are sending a file.

16. Click the **Cancel** button to disregard your settings.

    -or-

    Click the **OK** button to begin file transfer.

Sending and Receiving CMS/VM Files

OC://WebConnect Pro allows you to transfer files between a Java client and the Virtual Machine/Conversational Monitor System (VM/CMS) SNA application. You can use the Java client's **Transfers** menu for transferring files to suit your needs.
To transfer files between your directory system and a VM/CMS application

1. Make sure OC://WebConnect Pro is connected to a desired SNA host and VM/CMS application.

2. Select **File Transfer** from the **File** menu.

3. Select **INDFILE** from the **File Transfer** menu.

4. Select either **Send to Host** or **Receive from Host** from the **INDFILE** submenu.

5. Select the **CMS/VM** option.

6. Click the **Local File** button to search for the peer's file. A file selection window displays. The procedures for searching for the peer file name vary with your system. After you select the peer file, the name displays in the text field to the right of the **Local File** button.

7. Click the **UNIX Format** button if you want to transfer files in UNIX format. This allows line separators to be converted to carriage return and line feed pairs during a Send operation. During a Receive operation, carriage return and line feed pairs are converted to line separators.

8. Type a host file name in the **VM File Name** field in the **File Attributes** area. The VM file name can be from 1–8 characters in length.

☞ **Note:** The VM/CMS application automatically creates the receiving host's file name if a file name does not exist.

9. Type the appropriate file type in the **VM Filetype** field. The filetype parameter identifies the VM/CMS disk file type.

10. Type an appropriate value in the VM Filemode text box. The filemode parameter identifies the VM/CMS disk file mode. If you do not enter a filemode parameter, the VM/CMS application uses the A1 default value.

11. Select a transfer option from the **General** box in the **Transfer Options** area. The **Transfer Options** parameters allow you to configure the way the file's contents are treated during the transfer process. The choices are described below:

APPEND	This option allows you to append a local file to the end of an SNA host file; otherwise, you can append an SNA host file to a local file. The Append option overrides any other values specified by the Logical Record Size parameter and Record Format options.
ASCII	This option instructs the SNA host to translate data between the EBCDIC and ASCII character formats. You can use this option for translating ASCII formatted files, such as text edit files or print files.
CRLF	This option (by using the Send dialog) instructs the SNA host to replace the local file line separators with SNA record separators. If you use the Receive dialog, the SNA host replaces the SNA record separators with local file line separators. If you do not specify the CRLF option in the Send mode, the SNA host disregards the local file’s line separators.

Note: If you do not activate the Append option in the Receive dialog box, the SNA host file replaces the Java client file. If you do not activate the Append option in the Send dialog box, the TCP/IP host file replaces the SNA host file.

Caution

Do not use the ASCII or CRLF options for binary data (such as output data from a data base program) or object code files (such as C compiler object code). If the CRLF option is activated for a binary file transfer, unexpected results are produced when the file is used.

12. Select a record format parameter for the SNA host file from the **Format** box in the **Transfer Options** area. The **Format** check boxes specify the record format of the SNA host file. This is only valid if you are sending a file. The choices are described below:

Fixed	Indicates that the data set’s records are fixed-length
Variable	Indicates that the data set’s records are variable-length
None	Indicates no record format is selected

13. Type a logical record length of the SNA host file in the **Logical Record Size** field in the **Transfer Options** area. The parameter value represents the number of characters for each record. If the parameter is not entered, the record length is determined by the file transfer operation. For new files, the parameter ’s default value is 80. This is valid only if you are sending a file.

If you are replacing a file or appending information to a file, the characteristics of the existing file are used. If you are transferring variable length records, the parameter represents the maximum record size. If you do not send a record of the maximum operating system size, the parameter's value becomes the longest record sent.

14. Click the **Cancel** button to disregard your settings.

    -or-

    Click the **OK** button to begin file transfer.

Chapter 15: Security Overview

Overview

OC://WebConnect Pro provides a number of advanced features which can be utilized to securely deploy sessions on Intranets or the public Internet. These features can be utilized in various combinations to enable varying levels of security.

The main areas of concern dealing with security in OC://WebConnect Pro are listed below:

- Data privacy (encryption)
- Data integrity (message authentication)
- Firewalls and network topology
- Authentication of client to server
- Authentication of server to client

It is important to establish a desired overall network topology and security requirements criteria before starting to configure OC://WebConnect Pro. For example, will a firewall be used and will sessions on the internal network require encryption. OC://WebConnect Pro can be designed into a network topology with or without firewalls and also has the capability of running encrypted and non-encrypted sessions simultaneously. Knowing the security/topology requirements before you go on allows for a simpler OC://WebConnect Pro installation and customization. Security administration for OC://WebConnect Pro is done entirely at the server. No client administration is required.

If *server authentication* is a requirement, typically a concern when deploying over a public network, then the Secure Socket Layer (SSL) option should be used. Server authentication in SSL is provided via X.509 certificates. SSL also provides *Message Authentication* to prevent message tampering. There are many more benefits to using SSL which will be discussed later.
Client authentication is provided through a token passing mechanism. This mechanism relies on the customer's existing security between the browser and Web server, providing a method to re-authenticate a client before granting sessions.

Two types of message encryption between the OC://WebConnect Pro server and the client are provided. They cannot be used simultaneously:

SSL	Netscape Communications, Inc.	A choice of 6 cipher suites (also includes the RC4 algorithm)
		Client/Server encryption algorithm negotiations
RC4	RSA Data Security, Inc.	40 bit encryption key*
		128 bit encryption key (128-bit encryption is Export Restricted, US Only)

Note: OC://WebConnect Pro qualified for ECCN 5D002 general license exemption TSU (Technology and Software Unrestricted) per mass market notes. This ruling indicates that individual licenses are only required for Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria.

Firewalls and network topology

The multi-tier security approach in OC://WebConnect Pro is designed to complement existing internet security, not replace firewalls and other security devices. Due to the many types of firewalls which can be deployed in various configurations, we cannot discuss all the possibilities here. In general, OC://WebConnect Pro works with Proxy Firewalls when a hole is punched in the firewall to allow the connection.

Limitations

- OC://WebConnect Pro does not work with Masquerade Firewalls.
- If OC://WebConnect Pro is behind a firewall and the client is behind a different (Proxy) firewall, this configuration will not work properly.

The Admin port must be protected to operate the SSL and client token authentication features securely.

The ultimate protection is to have the Web server and OC://WebConnect Pro on the same machine and to use the local host for the IP address of the Admin port. In this way messages never leave the machine. The OC://WebConnect Pro session is the focal point of security.

Protecting Host Resources

In OC://WebConnect Pro, the point of access to host resources is through session definitions. For instance, host name, port and LU are all components of a session definition. By using the access protection of the Web server you can restrict access to a given session. In addition, by using the *client authentication* feature the users security is propagated into OC://WebConnect Pro to protect session access.

For example, the Web server could authenticate the user, and then present different choices depending on who the user is. Individual users or groups could be confined to use certain session definitions mapping to specific host resources. By linking the token to the session definition, the authentication and mapping defined on the Web server is extended to and enforced by the OC://WebConnect Pro server.

SSL cipher suites are set on a per session basis. This allows the configuration of different cipher suites on different sessions. The *SSL Required* option requires the user to use SSL (via secure Java port) when accessing a session with this option set. If the *SSL Required* option is not set, then SSL is optional for the session.

SSL Versus RC4

Two types of encryption are available between the OC://WebConnect Pro Java client and the OC://WebConnect Pro server. For a particular session, only one type of encryption can be used at a time.

SSL-enabled applets take longer to download. This is due to the fact that SSL capabilities in today's browsers are not accessible to applets; therefore, SSL libraries must be included and downloaded with the applet. Once downloaded, a session will set up quicker using the SSL option than a session using RC4 with Diffie-Hellman. For keys less than 1024, SSL sessions will also use significantly less server CPU during session startup.

SSL may have varying levels of performance dependent on the particular cipher suite implemented. Cipher suites utilizing RC4 encryption and the MD5 hashing algorithm will yield the highest performance.

The RC4 encryption option allows for a quicker applet download time since it uses a smaller applet, however it takes longer to setup a session (due to the Diffie-Hellman algorithm used for key generation).

Also, the server CPU load for session startup is generally higher. There is no specific performance data on RC4 vs. SSL for large numbers of clients, however it is a logical assumption that RC4 will run quicker than SSL since SSL adds padding and performs message authentication.

On the Client side, SSL should not be perceptible. On the server, unless the server becomes CPU bound, SSL will not cause a degradation in performance.

Detailed discussions of the OC://WebConnect Pro SSL and RC4 implementations can be found later in this chapter. For additional technical information on SSL and RC4, refer to the following Web sites:

- SSL – http://search.netscape.com/newsref/std/sslref.html
- SSL – http://www.netscape.com/ and do a search on "SSL"
- RC4 – http://www.rsa.com/

SSL is recommended for deploying OC://WebConnect Pro over the public internet. The RC4 with Diffie-Hellman option is intended more for intranet use.

SSL in OC://WebConnect Pro

OC://WebConnect Pro uses SSL to secure connections between an OC://WebConnect Pro Java client and the OC://WebConnect Pro server without requiring any special configuration on the client machine. This is achieved by leveraging the SSL provided in the customer's Web server and browser. That is, security parameters are passed to the OC://WebConnect Pro Java client over the browser-to-Web server connection.

When the browser requests an OC://WebConnect Pro session from the Web server, a process on the back end of the Web server will connect to the OC://WebConnect Pro server and obtain the configuration parameters for the client session. Included in these parameters are the SSL port on the OC://WebConnect Pro server, the cipher suite to be used for the session, and a hash, or fingerprint, of the OC://WebConnect Pro server certificate. This fingerprint is later used to verify the certificate received from the OC://WebConnect Pro server during SSL negotiations, thereby authenticating the OC://WebConnect Pro server.

OC://WebConnect Pro uses an alternate port for SSL connections so that different security measures can be applied to the SSL and non-SSL ports. For instance, an installation of OC://WebConnect Pro could choose to hide the unsecured port behind the corporate firewall but expose the SSL port to internet traffic.

A key pair must be generated for OC://WebConnect Pro. The private key is password protected and used only by OC://WebConnect Pro. An X.509 Certification Authority certifies the public key. The resulting certificate is used by clients to authenticate the server as part of the SSL protocol. Before enabling SSL in OC://WebConnect Pro you should have previously installed a private key and certificate for the server. Please see information on Key Pairs and X.509 Certificates below.

Cipher Suites

SSL defines a Handshake Protocol for negotiating a "Cipher Suite" and allowing the client and server to authenticate each other. The cipher suite specifies the algorithms to be used for peer authentication, data encryption, and message authentication when normal session traffic begins. The actual algorithms defined by a cipher suite are independent of the SSL protocol.

OC://WebConnect Pro supports several popular encryption algorithms, such as DES, Triple DES, and RC4. The RSA public-key algorithm is used for both key exchange and peer authentication. Secure Hash Algorithm (SHA-1) and MD5 are supported for message authentication.

A separate cipher suite can be selected for each configured session. Cipher suites are set from the security section of session configuration using the GUI or HTML configuration.

Key Pairs and X.509 Certificates

SSL utilizes public-key cryptography for peer authentication and key exchange. OC://WebConnect Pro uses the RSA public-key algorithm for both of these functions. The server’s public key is given to the client in a digital certificate (X.509 standard). The client generates a master secret to be used to derive a session key for data encryption. The client then encrypts the master secret with the server’s public key and sends it back to the server. Now the server can decrypt the master secret and communicate with the client using the encryption algorithm specified in the negotiated cipher suite.

This all requires that a key pair be generated for the server. The private key must be kept secret, only to be used by the server. The public key is given to an X.509 Certification Authority (CA) for certification.

The CA generates a certificate containing the server’s name and public key, the CA’s name, validity dates, and a serial number for the certificate. Finally, the CA "signs" the certificate with its own private key, so that its authenticity can be verified by anyone in possession of the CA’s public key.

An SSL client authenticates an SSL server by verifying the signature in the server certificate with the public key of the CA specified in the certificate. For this to work, the client must have ready access to the CA’s certificate.

If configured to do so, an SSL server may request a certificate from the client so that the server also may authenticate the client. HTML extensions exist to trigger a browser to generate a key pair, request a certificate, and accept a certificate for installation. This allows a browser to operate with a Web-based CA. Netscape and Microsoft, both support this type of browser configuration under user control.

Whether you choose to use a trusted third party for your CA, or whether you establish a private CA within your company or organization will probably depend on who the targeted users of your system will be and the level of security you require.

If your users will typically be anonymous or outside of your administrative control, or if your security requirements are not stringent, you will probably want to use a certificate issued by a trusted third party. On the other hand, if you want the highest level of security possible, you will probably want to establish a private CA within your company or organization, using third party certification tools, such as Netscape Certificate Server, Entrust Web CA, or XCERT Sentry CA. Then you can issue your own certificates for servers and clients, and configure them to honor your certificates and only your certificates.

To use SSL securely in OC://WebConnect Pro, you will need to launch the OC://WebConnect Pro Java applets from a secure Web server using an SSL-enabled browser. The Java applet will then connect to the Secure Java Port of the OC://WebConnect Pro server, using the SSL protocol and authentication data passed in over the SSL-protected browser-to-Web server connection.

The OC://WebConnect Pro server must have a key pair and certificate before you can use the SSL feature. These are normally generated during the server installation process, but can be generated later using the configuration utility. Since server authentication data is passed to a Java applet over the secure browser-to-Web server connection, it is not necessary for a known CA to issue the OC://WebConnect Pro server certificate. You can choose to allow OC://WebConnect Pro to generate its own certificate, or if you prefer, you can have it generate only a PKCS #10 certificate request to be submitted to your CA.

If you choose to use a CA to provide the certificate for the OC://WebConnect Pro server, it will need to be manually installed.

The server certificate should be a base64-encoded, DER-formatted, X.509 certificate, stored in a file called cert.txt in the security subdirectory. This should be a concatenation of the server’s certificate, the issuer’s certificate, plus any others in the hierarchy if the issuer is not the root CA. They should be ordered server certificate first, root CA certificate last. You may need to cut and paste from two or more files to create cert.txt.

Limitations

- Limited to Cipher suites provided.
- 128 bit encryption is Export Restricted.
- Cannot be used in conjunction with the RSA RC4 encryption option.

Dependencies

For complete security, an SSL enabled Web browser and Web server must be used.

Cipher Suites

Non-Exportable Cipher Specifications Table

RSA_WITH_RC4_128_SHA

- RSA algorithm for key exchange and peer authentication.
- RC4 128-bit encryption.
- SHA (Secure Hash Algorithm) for message authentication.

RSA_WITH_RC4_128_MD5

- RSA algorithm for key exchange and peer authentication.
- RC4 128-bit encryption.
- MD5 algorithm for message authentication.

RSA_WITH_3DES_EDE_CBC_SHA

- RSA algorithm for key exchange and peer authentication.
- Triple DES encrypt-decrypt-encrypt (EDE) encryption, in cipher block chaining (CBC) mode.
- SHA (Secure Hash Algorithm) for message authentication.

RSA_WITH_DES_CBC_SHA

- RSA algorithm for key exchange and peer authentication.
- DES encryption in cipher block chaining (CBC) mode.
- SHA (Secure Hash Algorithm) for message authentication.

Exportable Cipher Specifications

RSA_EXPORT_WITH_RC4_40_MD5

- RSA algorithm for key exchange and peer authentication.
- RC4 40-bit encryption.
- MD5 algorithm for message authentication.

RSA_EXPORT_WITH_DES40_CBC_SHA

- RSA algorithm for key exchange and peer authentication.
- DES 40-bit encryption in cipher block chaining (CBC) mode.
- SHA (Secure Hash Algorithm) for message authentication.

SSL Protocol with No Encryption

RSA_WITH_NULL_MD5

- RSA algorithm for peer authentication.
- MD5 algorithm for message authentication.

RSA_WITH_NULL_SHA

- RSA algorithm for peer authentication.
- SHA algorithm for message authentication.

RC4 Encryption Option

The RC4 option uses the Diffie-Hellman algorithm for key generation at the time a connection is made. The RC4 encryption option and key length is set on a per session basis. Since an inherent limitation of RC4 is that it is susceptible to Man-in-the-middle attacks, this option is best for Intranets.

Limitations

- Only the 40-bit RC4 encryption is available in the Ultra Lite applet.
- Cannot be used in conjunction with the SSL encryption option.
- When RC4 is configured for a given session, then it is always required for that session.

Client Authentication (token)

The *token authentication* feature in OC://WebConnect Pro is a user authentication mechanism that leverages the existing security infrastructure of the customer’s Web server/browser environment. The concept is that the OC://WebConnect Pro server dynamically generates tokens, delivered to the browser along with the OC://WebConnect Pro applet, to allow the applet to gain access back to the OC://WebConnect Pro server. The result is that the OC://WebConnect Pro installation is brought transparently under the umbrella of the customer’s existing authentication scheme, incurring no additional administrative overhead. To be 100% effective, SSL must be running between the Web server and browser, so that tokens are secure from outside snooping.

How it Works

An OC://WebConnect Pro user will use his browser to first connect to a home page or logon screen on the Web server. The user’s HTML will present a button or link to allow the user to request an OC://WebConnect Pro session. OpenConnect provides functional HTML pages with the product that can be used as distributed or as an example for development of custom HTML.

As a result of clicking this button, the OC://WebConnect Pro CGI-BIN is invoked. The CGI-BIN will connect to the admin port of the OC://WebConnect Pro server and request the applet parameters. The server will respond with HTML-formatted parameters intended to start up a java applet. Among other things, these parameters include the applet name/location, the name and port of the OC://WebConnect Pro server and a session name used by the server to identify host information and session attributes. If the *token authentication* feature has been enabled in the server, an additional parameter will be supplied to the applet: a token.

This HTML, containing the applet parameters, is passed back through the Web server to the browser. The browser requests the server to send down the specified applet, then invokes this applet under the control of the resident JVM, passing in the parameters originating from the OC://WebConnect Pro server. Finally, the applet connects to the OC://WebConnect Pro server, which in turn connects to the host, and the user session commences. If the applet has received a token, it must present this token to the server during the initial handshake (within a configured timeout period), or else the session will be rejected.

It is very important that the Admin port for OC://WebConnect Pro remain behind the firewall, or on a private network, and not be exposed to the Internet or other unsecured network. Tokens would be accessible to anyone on these networks.

In OC://WebConnect Pro, the point of access to host resources is through session definitions. For instance, host name, port and LU are all components of a session definition. Linking the token to a session effectively propagates any access protection present in the customer's HTML to the OC://WebConnect Pro environment.

For example, the Web server could authenticate the user, and then present different choices depending on who the user is. Individual users or groups could be confined to use certain session definitions mapping to specific host resources. By linking the token to the session definition, the authentication and mapping defined on the Web server is extended to and enforced by the OC://WebConnect Pro server, thus protecting host resources.

Operation of the Token Authentication Feature in OC://WebConnect Pro Server

When the *token authentication* feature is enabled on the server, it is enabled for all sessions on the server. In addition to the on/off switch, the administrator is able to specify a time-to-live value in seconds. The default value is 90 seconds.

The *token authentication* feature uses a pseudo-random number generator powered by the MD5 hashing algorithm to generate the tokens (16 bytes long). A token is generated each time a request is received for applet parameters over the Admin port. The server keeps a copy of the token, which is given a time stamp and marked with the name of the session.

When the applet connects to request a session, it must present its token to the server. The server searches its list of active tokens for a match, discarding expired tokens along the way. If the token is found, the server verifies that the session matches, then discards the token.
If the server cannot find a token or if a session mismatch is detected, the client is disconnected and a descriptive error message is written to the system log, including the port and address of the offending client. The server also logs the occurrence of timed-out tokens.

For applets wishing to establish additional sessions, for instance, in response to selecting *New* from the file menu, protocol exists between the client and OC://WebConnect Pro server to allow an existing authenticated session to request a new token.

Limitations

- This feature will not work with a channel-type Web architecture such as Marimba.
- This feature will not be immediately available for OpenVista.
- The Admin Port must be protected.

Dependencies

In order for this feature to be effective, a secure link must be provided between the Web server and the client browser.

SSL should be enabled between the client browser and OC://WebConnect Pro in order to protect the token when requesting a session.

This feature will not work with any other OC://WebConnect Pro implementation relying on static HTML pages for applet launching. A live connection must be made from the Web server to the OC://WebConnect Pro server to fetch the token. A CGI-BIN is provided with the product for performing this function.

Security Questions

Where can I get more information on SSL and RC4?

Both Netscape and RSA have Web sites where more information is available.

For more information on SSL, refer to:

http://search.netscape.com/newsref/std/sslref.html
http://www.netscape.com/ - and do a search on “SSL”.

More information on RC4 from RSA Data Security Inc. can be found at:

http://www.rsa.com/

What if I want to get my own certificate?

An alternative is to use a CA product, such as Netscape Certificate Server, Entrust Web CA or XCert Sentry CA. These products will all generate keys and certificates for their secure Web servers, and can generate a certificate for the OC://WebConnect Pro certificate request.

It is recommended that customers use the third party CA or CA product to generate the certificate for the secure Web server only, and let OC://WebConnect Pro generate its own certificate—it is much less trouble and no less secure. OC://WebConnect Pro always generates its own keys and certificate request, so there is no increase in security by having a third party certify the request.

Chapter 16: National Language Support

Overview

OC://WebConnect Pro provides National Language Support (NLS) and other localization features for the administrator on the server side and for the end user. Server languages are totally independent from the individual client session languages allowing for true international use of this product. The localization features are divided into four categories; server language support, language for each client session, target host code page for the session, and keyboard support.

OC://WebConnect Pro Server Language Localization

OC://WebConnect Pro can be configured to one of four possible server languages. The OC://WebConnect Pro server language is used for the HTML configuration pages, the GUI (graphical) Configurator client, the OC://WebConnect HTML session selection pages, and the online user guide. When the server language is changed the HTML files provided with OC://WebConnect Pro will automatically be updated which will include any previous configured server host names or ports.

The server language will be used for all administrator interaction and associated help displays with this OC://WebConnect Pro server.

Four server languages are available for system administration:

- US English
- French
- German
- Spanish

To select the server language as part of the install process, select function number seven, (7) *Configure Default Administration Language,* from the configure menu. Then select the appropriate number for the language you want to use for server administrative functions and press RETURN. Refer to the *OC://WebConnect Pro Installation Guide* for more detail instructions.

To change the server administration language after initial installation, use the OC://WebConnect Pro configuration utility. Select function number seven, (7) *Configure Default Administration Language,* from the utility menu. Then select the appropriate number for the language you want to use for server administrative functions and press RETURN. For more information, see *Chapter 5: Server Administration and Configuration*.

OC://WebConnect Pro Client Language Localization

The language for the client is chosen as part of the session setup. The language chosen will be used for all client generated messages, information displays, and menus at the client emulator window. The available languages are shown below along with the code used internally to represent that language. The chosen language is not related to the content or format of the data displayed in the emulator session.

Language/Country	Internal code
US English	en_US
UK English	en_GB
French	fr_FR
German	de_DE
Italian	it_IT
Swiss/German	de_CH
Norwegian	no_NO
Dutch	nl_NL
Castilian Spanish	es_ES
Portuguese/Brazil	pt_BR
Swedish	sv_SE
Turkish	tr_TR
Japanese	ja_JP
Chinese Traditional	zh_TW
Chinese Simplified	zh_CN

The client language is chosen from either the **HTML Administration and Configuration** or **GUI Configurator.** See *Chapter 5: Server Administration and Configuration*.

Changing the Client Language Using HTML Configuration

Select the Configuration link on the main OC://WebConnect Pro HTML page and enter the Administrator Password. Choose the session you wish to edit or create a new session. Selecting Edit, Copy or New will automatically link you to the selected Configuration page. From this page, link to the Display Page using the left hand buttons. Highlight the desired client language and either press return or use the left mouse click to select the highlighted language. This same page can be used to set other localized parameters as defined in this chapter.

Changing the Client Language Using the GUI Configurator

Select the GUI Configurator link on the main OC://WebConnect Pro HTML page and enter the Administrator Password. Select the sessions tab and then choose the session you wish to edit by selecting Properties or create a new session by selecting Create. Select Display Settings and highlight the desired client language and either press return or use the left mouse click to select the highlighted language. This same page can be used to set other localized parameters as defined in this chapter.

OC://WebConnect Pro Target Host Code Page Support

Each target host has identified a code set and an associated code page. This code set and code page may be the system chosen default, but it does exist. For MVS systems in the United States the default code set is 697 and the code page is 37. The code set is the defined set of graphic characters supported. In the code set 697 example there is a graphic for the dollar sign, but no graphic for the pound-sterling-sign. The code page defines an encoding structure for each graphic in the code set. In code page 37 the graphic for the dollar sign is represented by the hexadecimal code of 5B. In code page 285 (UK English) the pound-sterling is represented by the same code point (5B). OC://WebConnect Pro only requires knowledge of the code page.

Language support and code page support are not related in OC://WebConnect Pro Version 3.1 and above. Language is used to identify the character strings displayed for operation of the client and configuration of the server. The code page is used to transform the target host data into Unicode equivalents. The client can function using the Italian language and the Swedish code page or the French language and the Chinese code page or any other combination.

When a session is defined for OC://WebConnect Pro, a target system code page number is defined. For convenience, the most prevalent code page for the client session language is displayed for a default. The administrator may change this value. The defaults displayed are shown below:

Language/Country	EBCDIC Default Code Page	VT Default Code Page
US English	37	819
UK English	285	819
French	287	819
German	273	819
Italian	280	819
Swiss/German	500	819
Swiss/French	500	819
Norwegian	277	819
Dutch	37	819
Spanish	284	819
Portuguese/Portugal	37	819
Portuguese/Brazil	37	819
Swedish	278	819
Turkish	1026	920
Japanese	290,1027,300	33722
Chinese Traditional	937	964
Chinese Simplified	935	1383
Korean	833,834	no support

The client emulator window always uses code page 13488 (Unicode UCS-2 level 1).

The programming mechanism to convert from the host code page to the emulator code page, and back, is called the transform type. OC://WebConnect Pro includes six transformation types. The purpose of having different transformation types is to reduce the size of translate tables, decrease the time to perform translations, or to reduce the amount of data sent between server and client. The transform types are described below:

Configuration Title	Internal code	Description
Single Byte to/from Single Byte	sbonly	Classic single byte translation table. The input code page is transformed to single byte ASCII Latin 1. The ASCII Latin 1 is mapped to the first 256 Unicode positions.
Single Byte to/from Unicode	sbcs	The single byte code page is transformed into its appropriate Unicode character. Supports all of the Latin XX and special characters. Unicode (2 bytes per character) is transmitted between server and client.

Configuration Title	Internal code	Description
Single/Multi-byte to/from Unicode (Multiple Tables)	sbmb	Multiple tables are used to transform single byte EBCDIC characters into Unicode. Another single table is used to transform EBCDIC double byte into Unicode. This is used when Asian code page rotate is supported. Unicode is transmitted between server and client.
Single/Multi-byte to/from Unicode (Single Table)	mixed	A single table is used transform EBCDIC Asian single and double byte into Unicode. This is much more efficient than multiple tables, but cannot rotate. Unicode is transmitted between client and server.
Enhanced UNIX code to/from Unicode	euc	Used to transform from Asian UNIX EUC host representation into Unicode. Unicode is transmitted between client and server.
UNIX PC Code to/from Unicode	pc	Used when the Asian UNIX host is encoded with a PC encoding scheme. Unicode is transmitted between client and server.

The transform tables are very large, so only selected tables are shipped to represent the languages and transform type supported. The shipped tables are listed below:

Language	Code Page	Conversion	Comments
US English	037	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
Netherlands	037	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
Portugal	819	none	ASCII is mapped to Unicode at the client
Brazil			
UK	285	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	285	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
France	297	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	297	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
Germany	273	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	273	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
Italy	280	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	280	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode

Language	Code Page	Conversion	Comments
Switzerland	500	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	500	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
Norway	277	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	277	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
Spain	284	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	284	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
Sweden	278	Single Byte to/from Single Byte (sbonly)	EBCDIC/ASCII
	278	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode
Japan	290	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC Katakana single byte / Unicode
	1027	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC Latin 1 single byte / Unicode
	300	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC Double byte / Unicode
	942	UNIX PC to/from Unicode	ASCII PC mixed (1041 + 301) / Unicode
	33722	Enhanced UNIX code to/from Unicode	EUC (895 + 952 + 896 + 953) / Unicode
Korea	833	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC single byte / Unicode
	834	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC double byte / Unicode. **Note:** This table is provided algorithmically. UNIX is not supported for Korean.

Language	Code Page	Conversion	Comments
Simplified Chinese	836	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC single byte / Unicode
	837	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC double byte / Unicode
	935	Single/Multi-byte to/from Unicode (Single Table)	EBCDIC mixed (836 + 837) / Unicode
	1381	UNIX PC to/from Unicode	ASCII PC mixed (1115 + 1380) / Unicode
	1383	Enhanced UNIX code to/from Unicode	EUC (367 + 1382) / Unicode
Traditional Chinese	037	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC single byte / Unicode
	835	Single/Multi-byte to/from Unicode (Multiple Tables)	EBCDIC double byte / Unicode
	937	Single/Multi-byte to/from Unicode (Single Table)	EBCDIC mixed (037 + 835) / Unicode
	948	UNIX PC to/from Unicode	ASCII PC mixed (1043 + 927) / Unicode
	964	Enhanced UNIX code to/from Unicode	EUC (367 + 960 + 961) / Unicode
Turkey	1026	Single Byte to/from Unicode (sbcs)	EBCDIC/Unicode
	819	none	ASCII/Unicode

Code page rotate is a capability of OC://WebConnect Pro used mostly to support the rotation of code pages between Japanese Latin 1 EBCDIC and Japanese Katakana EBCDIC. The function is mapped to a keystroke using the function **RotateCP**. The default keystroke is Ctrl-F5. The keymap entry is **RotateCP=<Control+F5>**.

The function is effective only for "Single Double Byte to/from Unicode (Multiple tables)" type transforms. It is automatically activated when more than one single byte code page is coded in the code page field. The rotation occurs between the single byte tables, the last entered code page number is the double byte table. When the RotateCP key is pressed the code page is changed to the next page in rotation, then, the entire screen data it re-transformed and transmitted.

The target host code page number and the transform type are chosen from either the **HTML Administration and Configuration** or **GUI Configurator.** (See *Chapter 5: Server Administration and Configuration*) .

Changing the Transform Type Using the HTML Administration and Configuration

Select the Configuration link on the main OC://WebConnect Pro HTML page and enter the Administrator Password. Choose the session you wish to edit or create a new session. Selecting Edit, Copy or New will automatically link you to the selected Configuration page. From this page, link to the Display Page using the left hand buttons. Highlight the desired host code page number and either press return or use the left mouse click to select the highlighted code page. Similarly, highlight the transform type required to support the desired language conversion as stated in the above tables.

Changing the Transform Type using the GUI Configurator

Selecting the GUI Configurator link on the main OC://WebConnect Pro HTML page and enter the Administrator Password. Select the sessions tab and then choose the session you wish to edit by selecting Properties or create a new session by selecting Create. Select Display Settings and highlight the desired host code page number and either press return or use the left mouse click to select the highlighted code page number. Similarly, highlight the transform type required to support the desired language conversion as stated in the above tables.

OC://WebConnect Pro Keyboard Considerations

OC://WebConnect Pro provides a key mapping facility. This facility is provided to allow emulator specific keys to be mapped to a platform specific key. For example, the 3270 clear key can be mapped to the PC Ctrl plus A key. The key mapping function also allows the mapping of certain specific international keys to their proper codes. A sample international keymap is provided (natl3270.kbm) which will support keyboards in all supported locales.

If you must add a new or different keyboard layout the following information will aid you.
Many international keyboards have characters in different locations than their US counterparts. The different locations are mapped for OC://WebConnect Pro by the Java virtual machine and are transparent to OC://WebConnect Pro. In addition, some keys on international keyboards are typed by using an **alt-Gr** key. Normally the **alt-Gr** key replaces the right **Ctrl** key of the US keyboard. Java presents keys typed by the **alt-Gr** key to OC://WebConnect Pro as the desired key with a **Ctrl** modifier.

If the requested key is represented by a Unicode value greater than 128 the **Ctrl** modifier is ignored by OC://WebConnect Pro. This handles the great majority if international characters. A set of characters is represented by a Unicode value less than 128 and keyed on certain international keyboards using the **alt-Gr** key. Then an entry must be added to the keymap to represent that key. If no keymap entry is made, OC://WebConnect Pro treats the key as a **Ctrl-**modified key with no map and ignores the key. The **Ctrl-**modified key is mapped to itself.

Example: The at sign (@) is represented in Unicode as decimal 64 (X0040). On the French keyboard the at sign is typed by holding the alt-Gr key and pressing the zero (0) key. In the OC://WebConnect Pro Java code, if the at sign (@) plus **Ctrl** is not mapped, it is ignored. The following line in the keymap file corrects the situation:

```
0040=<Control+at>
```

This line tells the Java client to replace the at (@) character with hexadecimal 40 (the at character) when the control key is also present.

OC://WebConnect Pro includes sample international mappings for 3270 (**natl3270.kbm**), 5250 (**natl5250.kbm**) and VT (**natlvt.kbm**). The samples should be sufficient for most locales.
To assign a particular keyboard map to a specific client session number, use either the HTML configuration utility or the **GUI Configurator.** See *Chapter 5: Server Administration and Configuration*.

Changing the Keyboard Map Using HTML Configuration

Select the Configuration link on the main OC://WebConnect Pro HTML page and enter the Administrator Password. Choose the session you wish to edit or create a new session. Selecting Edit, Copy or New will automatically link you to the selected Configuration page. From this page, link to the Display Page using the left hand buttons. Highlight the desired keyboard map and either press return or use the left mouse click to select. This same page can be used to set other localized parameters as defined in this chapter.

Changing the Keyboard Map Using the GUI Configurator

Selecting the GUI Configurator link on the main OC://WebConnect HTML page and enter the administrator password. Select the **Sessions** tab and choose the session you wish to edit by selecting **Properties** or create a new session by selecting **Create**. Select **Display Settings** and enter the desired keyboard definition file name. This same page can be used to set other localized parameters as defined in this chapter.

OC://WebConnect Pro File Transfer Localization

In the Asian locales file transfer to TSO, CICS and VM is accomplished using the host function APVUFILE. APVUFILE supports the capabilities of IND$FILE in addition to new capabilities for the Asian market. APVUFILE allows optional inclusion of SI/SO in the transferred file. APVUFILE supports optional trailing blank elimination. APVUFILE most significantly supports transfer of double byte EBCDIC and translation into locale dependent data.

When files are transferred in ASCII mode using IND$FILE the conversion from/to ASCII is accomplished by IND$FILE host component. All translation is from/to Latin 1, therefore, the previously described additional translation is required. When files are transferred in ASCII (or JISCII) using APVUFILE, the conversion is accomplished by the off-host component (OC://WebConnect Pro in our case). OC://WebConnect Pro performs the conversion in two steps. First, the OC://WebConnect Pro server transforms the data from double byte EBCDIC to Unicode using the parameters supplied for the session (code page number and transform type). Second, the Java client uses the Java virtual machine to transform from Unicode into the platform specific encoding of files. The double translation can result in data inconsistencies when a character does not exist in Unicode, but is unavoidable in a Java environment.

The host name of the file transfer program is customizable. The default is IND$FILE. OC://WebConnect Pro automatically maps IND$FILE to APVUFILE for the supported Asian locales. If the customized name is not IND$FILE, the customized name will be used.

Chapter 17: OC://WebConnect Pro Print Solutions

Selecting a Print Solution

As an administrator, you can allow users to print a session screen and enable 3287 printing by selecting the **Print Settings** option on the **Sessions** tab in the **GUI Configurator** window. Choose between four options that works best for your environment, allowing users to print from an open session window and enables 3287 printing from a browser window. Printing options are listed below.

OC://WebPrint Option

This option allows full control over font size and style and “auto fits” the document based on page orientation. This option requires you to install OC://WebPrint locally on the client, and a program for installation is provided. OC://WebPrint is dependent upon the runtime environment, so if you switch from an Internet Explorer to a Netscape browser, you must install the appropriate OC://WebPrint libraries.

Operating Systems Requirements	Java Environment Requirements	Installation Requirements
Windows ’95 Windows NT	Internet Explorer 3.0 or 4.0 Netscape 3.0 or 4.0	Local installation required

Installing OC://WebPrint

1. From the main OC://WebConnect Pro 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 Web browser.

5. Execute **OCWebPrint.exe** and follow the prompts to install OC://WebPrint.

6. Restart your browser.

OC://WebPrint is now available for use with all OC://WebConnect Pro screen print and 3287 print functions.

JavaScript Print Option

Use the JavaScript Print option if you do not have access to the software required for the OC://WebPrint option. There is no software to install on the client. The JavaScript Print option provides quality printing because printing is performed by the browser.

Operating Systems Requirements	Java Environment Requirements	Installation Requirements
Windows '95 Windows NT Solaris	Netscape 3.x or 4.x Internet Explorer 4.01	No local installation required

JDK 1.1 Print option

The JDK 1.1 print solution using the Java solution built into all browsers which support JDK 1.1. No additional installation is required.

Operating Systems Requirements	Java Environment Requirements	Installation Requirements
Windows '95 Windows NT	Netscape 4.x with JDK 1.1 patch Internet Explorer 4.x HotJava 1.x	No local installation required

Printing a Screen

You can print a single session window after your administrator selects a print screen option.

1. From your open session window, select **Print Screen** from the **File** menu. The standard printer window for your system opens.

2. Follow the procedures for printing with your system.

Using 3287 Printing

You can print from your browser using the 3287 print session option after your administrator selects a print option. To print from your browser to a specific logical unit (LU) and gateway:

1. Select **3287 Print Session** from the **Select Sessions** window. A printer session window opens.
2. Make sure the correct gateway and LU displays in the printer session window. If not, reconfigure the **Host** and **Port Number** fields in the **Session Settings** on the **Session Properties** tab.
3. Send a mainframe print job to the selected LU. The print session window displays that the session is printing.

Notes

- To check the LU and gateway to which you are printing, select **Help Desk** from the **Help** menu on the printer session window that displays when you start a 3287 print session. A status window opens identifying printer information, such as the number jobs to print.
- To run print jobs unattended, disable the **Show Printer Dialog** from the **Settings** menu.

Appendix A: Glossary

3270 emulation

Imitation of an IBM 3270 computer terminal on a terminal connected to a TCP/IP computer so that the imitating system accepts the same data, executes the same computer programs, and achieves the same results as the imitated IBM terminal.

3270 session

The name given to a session when the TCP/IP computer is communicating with the host computer through the SNA3270 Presentation Services or 3270 TELNET Server.

3770 emulation

Imitation of an IBM RJE workstation on a terminal connected to a TCP/IP computer so that the imitating system accepts the same data, executes the same computer programs, and achieves the same results as the imitated IBM RJE workstation.

3770 session

The name given to a session when the TCP/IP computer is communicating with the host computer through the SNA3770 Presentation Services.

5250 emulation

Imitation of an IBM 5250 computer terminal on a terminal connected to a TCP/IP computer so that the imitating system accepts the same data, executes the same programs, and achieves the same results as the imitated IBM terminal.

API (Application Program Interface)

A language and message format used by an application program to communicate with the operating system or other system program such as a database management system (DBMS). APIs are implemented by writing function calls in the program, which provide the linkage to a specific subroutine for execution. Thus, an API implies that some program module or routine is either already in place or that must be linked in to perform the tasks requested by the function call.

Applet

A small Java program that can be embedded in an HTML page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The current rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

ASCII

American Standard Code for Information Interchange. A standard coded character set, consisting of 7-bit coded characters (8 bits including a parity check bit), used for information exchange among most non-IBM data processing systems, data communication systems, and associated equipment. The basic-ASCII character set contains English language characters. See EBCDIC and extended ASCII.

Attribute byte

The byte used to establish the characteristics of the field that follows it. For example, a byte that indicates that the following field is blinking, highlighted, or unprotected.

Browser

The program that serves as your front end to the World Wide Web on the Internet. In order to view a site, you type its address (URL) into the browser’s Location field; for example, www.computerlanguage.com, and the home page of that site is downloaded to you. The home page is an index to other pages on that site that you can jump to by clicking a **Click here** message or an icon. Links on that site may take you to other related sites.

Byte

A sequence of eight adjacent binary digits that are operated upon as a unit and that constitute the smallest addressable unit in the system.

Certificate Authority

An organization that issues digital certificates (digital IDs) and makes its public key widely available to its intended audience.

CGI (Common Gateway Interface)

A set of rules that describe how a Web server communicates with another piece of software on the same machine, and how the other piece of software (the “CGI program”) talks to the Web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard. Usually a CGI program is a small program that takes data from a Web server and does something with it, like putting the content of a form into an e-mail message, or turning the data into a database query. You can often tell that a CGI program is being used by observing **CGI-bin** in a URL

CGI-bin

The most common name of a directory on a Web server in which CGI programs are stored.

The **bin** part of **CGI-bin** is a shorthand version of **binary**, because executable versions of programs are sometimes called binaries. In real life, most programs found in **CGI-bin** directories are text files—scripts executed by binaries located elsewhere on the same machine.

Client

In the TCP/IP network environment, a process that employs (or consumes) resources provided by a server. Client is initiated by the user when issuing a networking command. The client process sends a request for service to a server process on the remote host. If the request is honored, a connection is established between the local client and the remote server processes. See Server.

Code page

A table that defines a coded character set by assignment of a character meaning to each code point in the table for a language or a country.

Configurator

The OC://WebConnect Pro automated, menu-driven utility used for customizing configuration files for the OC://WebConnect Pro server.

Configuration

(1) The arrangement of a computer system or network as defined by the nature, number, and the chief characteristics of its functional units. (2) The devices and programs that make up a system, subsystem, or network.

Daemon

A program running all the time on a UNIX system.

Digital Certificate

The digital equivalent to an ID card in the RSA public key encryption system. Also called digital IDs, digital certificates are issued by certification organizations after verifying that a public key belongs to a certain owner. The certification process varies depending on the certification authority (CA) that issues the certificates and the level of certification.

Domain Name

The unique name that identifies an Internet site. Domain Names always have two or more parts separated by a dot. The part on the left is the most specific, and the part on the right is the most general. A given machine can have more than one Domain Name, but a given Domain Name points to only one machine.

E-mail (Electronic Mail)

Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses (Mailing List).

Emulation

The imitation of all or part of one system by another so that the imitating system accepts the same data, executes the same programs, and achieves the same results as the imitated computer system.

Extranet

Business-to-business communications. A network that allows an organization's partners and suppliers to interact with corporate information and applications. This communication is typically done via a public or private switched network or virtual private network, VPN.

FAQ (Frequently Asked Questions)

FAQs are documents that list and answer the most common questions on a particular subject. FAQs are usually written by people who have tired of answering the same question over and over.

Firewall

A combination of hardware and software that separates a LAN into two or more parts for security purposes.

FTP (File Transfer Protocol)

A common method of moving files between two Internet sites. FTP is a special way to log in to another Internet site for the purpose of retrieving and/or sending files. Many Internet sites have established publicly accessible repositories of material that can be obtained using FTP by logging in with the account name **anonymous**; thus these sites are called anonymous FTP servers.

Gateway

(1) A functional unit that connects two computer networks or different network architectures. (2) A special purpose, dedicated computer that attaches to two or more networks and routes packets from one to the other.

Host

Any computer on a network that is a repository for services available to other computers on the network.

Host application subsystem

The host application subsystem is the program running on the host mainframe to and from which data is sent and received using the emulated station. Any VTAM application which supports 3270 display stations, 3770 RJEs, and printers (i.e., LU types 1, 2, and 3) can be accessed through the OC://WebConnect Pro server. For 3270 sessions, these host application programs include Customer Information Control System/Virtual Storage (CICS/VS), Information Management System (IMS), Time Sharing Option (TSO), and Virtual Machine/Conversational Monitor System (VM/CMS). For 3770 sessions, these host application programs include Job Entry Subsystem (JES) 2 and 3.

IBM channel. In the IBM System/370 and 370/XA architecture, the processor which does all of the actual input/output (I/O) processing.

HTML (HyperText Markup Language)

The coding language used to create Hypertext documents for use on the World Wide Web. HTML looks a lot like old-fashioned typesetting code, where you surround a block of text with codes that indicate how it should appear, additionally, in HTML you can specify that a block of text, or a word, is linked to another file on the Internet. HTML files are meant to be viewed using a World Wide Web Client Program, such as Netscape or Mosaic.

HTTP (HyperText Transport Protocol)

The protocol for moving hypertext files across the Internet. Requires a HTTP client program on one end, and an HTTP server program on the other end. HTTP is the most important protocol used in the World Wide Web (WWW).

Hypertext

Generally, any text that contains links to other documents - words or phrases in the document that can be chosen by a reader and which cause another document to be retrieved and displayed.

Internet (uppercase I)

The collection of independent and autonomous networks linked by gateways that use primarily the TCP/IP protocol suite and function as a single, cooperative virtual network.

internet (lowercase i)

Any time you connect two or more networks , you have an internet—as in international or interstate.

Internet address

The 32-bit address assigned to hosts on a TCP/IP internet.

Intranet

A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use. As the Internet has become more popular many of the tools used on the Internet are being used in private networks, for example, many companies have Web servers that are available only to employees. Note that an Intranet may not actually be an internet -- it may simply be a network.

IP Address (Internet Protocol Address)

The physical address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Client workstations have either a permanent address or one that is dynamically assigned for each dial-up session (see DNS). IP addresses are written as four sets of numbers separated by periods; for example:

204.171.64.2.

IP (Internet Protocol)

The TCP/IP standard protocol that defines the basic unit of information passed across an internet.

IP Routing

Protocol routing that provides a virtual connection from one TCP/IP-based LAN to another TCP/IP-based LAN through an SNA environment

Java

Java is a network-oriented programming language invented by Sun Microsystems that is specifically designed for writing programs that can be safely downloaded to your computer through the Internet and immediately run without fear of viruses or other harm to your computer or files.

JDK (Java Development Kit)

A software development package from Sun Microsystems that implements the basic set of tools needed to write, test and debug Java applications and applets.

JVM (Java Virtual Machine)

A Java interpreter from the JavaSoft division of Sun. It converts the Java intermediate language (byte code) into machine language one line at a time and then executes it. The Java Virtual Machine is licensed to software companies that incorporate it into their browsers and server software. Since it is used on all major platforms, Java programs run in "virtually" every computer. Microsoft also calls its Java interpreter a Java Virtual Machine.

Keyboard Mapping

The process whereby the Terminal Emulator maps the IBM 3270/3770 keys to the keyboard of the particular display station attached to the TCP/IP computer.

LU

Logical unit**.** In SNA, a port through which an end user accesses the SNA network in order to communicate with another end user and through which the end user accesses the functions provided by System Services Control Points (SSCPs).

LU 6.2

Provides a generalized facility for program-to-program communications. See APPC and LU type.

LU type

Shortened form for LU-LU session type. In SNA, the classification of an LU-LU session in terms of the specific subset of SNA protocols and options supported by the logical units (LUs) for that session. The SNA3270 Terminal Emulator supports LUs for display stations (LU type 2) and for printers (LU types 1 or 3). The SNA3770 Terminal Emulator supports LU type 1.

Plug-in

A piece of software that adds features to a larger piece of software. Common examples are plug-ins for the Netscape® browser and Web server. The idea behind plug-ins is that a small piece of software is loaded into memory by the larger program, adding a new feature, and that users need only install the few plug-ins that they need, out of a much larger pool of possibilities. Plug-ins are usually created by people other than the publishers of the software the plug-in works with.

Port

A place where information enters or leaves a computer, or both. On the Internet, port often refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers; for example, Web servers normally listen on port 80.

Protocol

A set of procedures or conventions used to formalize data transfer between points.

PU

Physical unit. In SNA, the component that manages and monitors the resources (such as attached links and adjacent link stations) of a node, as requested by an SSCP via an SSCP-SSCP session.

Security Certificate

A chunk of information (often stored as a text file) that is used by the SSL protocol to establish a secure connection. Security Certificates contain information about who it belongs to, who it was issued by, a unique serial number or other unique identification, valid dates, and an encrypted "fingerprint" that can be used to verify the contents of the certificate. In order for an SSL connection to be created both sides must have a valid Security Certificate.

Server

In a TCP/IP network environment, a process that provides resources to a network. The server is the remote host process that services the request made by the client. The server is a background process that listens for incoming service requests. When a server receives a request, it establishes a connection with the requesting client, spawns a subprocess, and returns to listening for more incoming requests.

Session

A logical connection between two stations that allows them to communicate.

SNMP (Simple Network Management Protocol)

A set of standards for communication with devices connected to a TCP/IP network. Examples of these devices include routers, hubs, and switches. A device is said to be "SNMP compatible" if it can be monitored and/or controlled using SNMP messages. SNMP messages are known as "PDU's" - Protocol Data Units. Devices that are SNMP compatible contain SNMP "agent" software to receive, send, and act upon SNMP messages.

SNA (Systems Network Architecture)

IBM's description of the logical structure, formats, protocols, and operational sequences for transmitting information units through and controlling the configuration and operation of networks.

SSL (Secure Sockets Layer)

A protocol designed by Netscape Communications to enable encrypted, authenticated communications across the Internet. SSL used mostly (but not exclusively) in communications between Web browsers and Web servers. URLs that begin with **HTTPS** indicate that an SSL connection will be used. SSL provides three important things: privacy, authentication, and message Integrity.

TCP/IP (Transmission Control Protocol/Internet Protocol)

(1) TCP provides a connection-oriented byte-stream service that is reliable and flow controlled. IP provides a connectionless datagram service that transparently forwards messages through the gateway. TCP is built on top of IP. TCP/IP protocols are defined by the Department of Defense Advanced Research Projects Agency (DARPA). (2) TCP/IP is also used synonymously for TCP/IP Application Suite. See TCP/IP Application Suite.

TCP/IP Application Suite

A collective term used for referring to DARPA-standard applications commonly distributed with the TCP/IP protocol. Two such applications are File Transfer Protocol (FTP) and Terminal Emulator Protocol (TELNET).

Telnet

(1) Acronym for teletype network. (2) A TCP/IP protocol used for remote login between hosts.

Terminal

A display station, RJE workstation, or printer.

Terminal emulator

In the OpenConnect Server, refers to either the SNA3270 Terminal Emulator or the SNA3770 Terminal Emulator. The OpenConnect Server’s SNA3270 Terminal Emulator provides IBM 3270 Information Display System emulation of IBM 3278 Display Stations, IBM 3278 Color Display Stations, and IBM 3287 Printers. The SNA3770 Terminal Emulator provides IBM 3770 Data Communication System emulation of the IBM 3776 Communication Terminals and IBM 3777 Communication Terminals. The 5250 TELNET Server terminal emulation emulates IBM 5250 midrange terminal types.

URL (Uniform Resource Locator)

The standard way to give the address of any resource on the Internet that is part of the World Wide Web (WWW).