

IBM Sterling Connect:Enterprise HTTP

Installation and Administration Guide

Version 1.4



This edition applies to the 1.4 Version of IBM® Sterling Connect:Enterprise® HTTP and to all subsequent releases and modifications until otherwise indicated in new editions.

Before using this information and the product it supports, read the information in *Notices*, on page 63.

Licensed Materials - Property of IBM

IBM® Sterling Connect:Enterprise® HTTP

© Copyright IBM Corp. 1999. 2011. All Rights Reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface

Task Overview	7
Conventions Used in This Guide	8
Sterling Connect:Enterprise HTTP Documentation	9

Chapter 1 **About Sterling Connect:Enterprise HTTP**

Sterling Connect:Enterprise HTTP Functions	12
--	----

Chapter 2 **Installing Sterling Connect:Enterprise HTTP**

Before You Begin	13
Installing Sterling Connect:Enterprise HTTP on the UNIX OS	14
Upgrading Sterling Connect:Enterprise HTTP on the UNIX OS	14
Installing Sterling Connect:Enterprise HTTP on Microsoft Windows	15
Upgrading Sterling Connect:Enterprise HTTP on Microsoft Windows	16
Uninstalling Sterling Connect:Enterprise HTTP from a Tomcat Web Server	16
Uninstalling Sterling Connect:Enterprise HTTP from a SunOne Web Server	17
Uninstalling Sterling Connect:Enterprise HTTP from IBM Websphere Web Server	17

Chapter 3 **Configuring the Servlet Engine**

Configuring the Tomcat Servlet Engine for Sterling Connect:Enterprise HTTP	19
Configuring the Tomcat Servlet Engine to Upgrade Sterling Connect:Enterprise HTTP	20
Configuring the Sun ONE Web Server	20
Configuring the IBM WebSphere Web Server	22

Chapter 4 **Configuring Security**

User Security	23
---------------------	----

	Data Security	23
	Cryptography.....	24
	Authentication	24
	Client-Server Session	24
	Obtaining a Certificate	25
	Creating the Key Certificate File.....	25
	Protecting Your SSL Passphrase.....	26
Chapter 5	Customizing Property Files	
	How Property Files Work.....	27
	The pfcheck Utility	28
	Configuring the SSL Property Files	28
	Customizing the System Property File	29
	System Property File Key/Value Pairs.....	30
	Customizing the Server Property Files.....	33
	Server Property File Key/Value Pairs	35
	Customizing the Remote Property Files.....	39
	Remote Property File Key/Value Pairs	40
	Customizing the Directory Property Files.....	42
	Directory Property File Key/Value Pairs	43
Chapter 6	Customizing the User Interface	
	Using the Change Password Function.....	45
	Customizing Your HTML Pages.....	45
	Redirecting Sterling Connect:Enterprise HTTP.....	47
	Localizing the User Interface	49
	Installing a Translation Package	49
	Available Translations	50
	Copying the Files	50
	Changing the Configuration.....	50
	Creating a New Translation	52
Chapter 7	Monitoring Sterling Connect:Enterprise HTTP	
	Logging Sterling Connect:Enterprise HTTP Activity.....	53
	Tracing Sterling Connect:Enterprise HTTP Activity.....	54
Appendix A	Error Messages	
	Logon Messages	57

Change Password Messages.....	59
Directory Messages.....	60
Send Messages	60
Receive Messages	61
Other Messages	62

Notices

Glossary

Index

Preface

The *IBM Sterling Connect:Enterprise HTTP Installation and Administration Guide* is written for the Sterling Connect:Enterprise system administrator who installs and configures IBM® Sterling Connect:Enterprise® HTTP and administers the system functions.

This manual explains how to install and configure Sterling Connect:Enterprise HTTP on the Microsoft Windows or UNIX operating system. It assumes that you have a working knowledge of Sterling Connect:Enterprise and all of the hardware and software components associated with it, and knowledge of Microsoft Windows and UNIX operating systems, including their major commands and functions.

Task Overview

The following table guides you to the information required to perform Sterling Connect:Enterprise HTTP tasks:

Task	Reference
Installing Sterling Connect:Enterprise HTTP on the UNIX OS	Chapter 2, <i>Installing Sterling Connect:Enterprise HTTP</i>
Upgrading Sterling Connect:Enterprise HTTP on the UNIX OS	Chapter 2, <i>Installing Sterling Connect:Enterprise HTTP</i>
Installing Sterling Connect:Enterprise HTTP on Microsoft Windows	Chapter 2, <i>Installing Sterling Connect:Enterprise HTTP</i>
Upgrading Sterling Connect:Enterprise HTTP on Microsoft Windows	Chapter 2, <i>Installing Sterling Connect:Enterprise HTTP</i>
Uninstalling Sterling Connect:Enterprise HTTP	Chapter 2, <i>Installing Sterling Connect:Enterprise HTTP</i>
Configuring the Tomcat Servlet Engine	Chapter 3, <i>Configuring the Servlet Engine</i>
Configuring the JRun Servlet Engine	Chapter 3, <i>Configuring the Servlet Engine</i>
Configuring the iPlanet Web Server	Chapter 3, <i>Configuring the Servlet Engine</i>
Configuring the IBM WebSphere Web Server for the UNIX OS	Chapter 3, <i>Configuring the Servlet Engine</i>
Configuring the IBM WebSphere Web Server for Microsoft Windows	Chapter 3, <i>Configuring the Servlet Engine</i>
Obtaining a key certificate	Chapter 4, <i>Configuring Security</i>

Task	Reference
Creating a key certificate file	Chapter 4, <i>Configuring Security</i>
Protecting your SSL passphrase	Chapter 4, <i>Configuring Security</i>
Configuring the SSL property files	Chapter 5, <i>Customizing Property Files</i>
Customizing System property files	Chapter 5, <i>Customizing Property Files</i>
Customizing Server property files	Chapter 5, <i>Customizing Property Files</i>
Customizing Remote property files	Chapter 5, <i>Customizing Property Files</i>
Customizing Directory property files	Chapter 5, <i>Customizing Property Files</i>
Customizing your HTML pages	Chapter 6, <i>Customizing the User Interface</i>
Redirecting Sterling Connect:Enterprise HTTP	Chapter 6, <i>Customizing the User Interface</i>
Localizing Sterling Connect:Enterprise HTTP	Chapter 6, <i>Customizing the User Interface</i>
Tracing Sterling Connect:Enterprise HTTP activity	Chapter 7, <i>Monitoring Sterling Connect:Enterprise HTTP</i>
Logging Sterling Connect:Enterprise HTTP activity	Chapter 7, <i>Monitoring Sterling Connect:Enterprise HTTP</i>

Conventions Used in This Guide

The *IBM Sterling Connect:Enterprise HTTP Installation and Administration Guide* uses certain notational conventions. This section describes the conventions used in this guide.

Convention	Description
lowercase letters	Lowercase letters or words in commands or syntax boxes require substitution by the user. For example, <code>PNODE=primary-node-name</code> indicates that you must provide the name of the primary node.
Underlined Letters	Underlining indicates default values for parameters and subparameters. For example, <code>RETAIN=Yes <u>No</u> Initial</code> specifies that the default for <code>RETAIN</code> is <code>NO</code> .
Vertical Bars ()	Vertical bars indicate that you can supply one of a series of values separated by the vertical bars. For example <code>HOLD=Yes No Call</code> specifies that <code>Yes</code> or <code>No</code> or <code>Call</code> is valid.
Italics	Italic letters are placeholders for information you must provide. Italic font also indicates book, chapter, and section titles and is used for emphasis in the text.
Punctuation	Code all commas and parentheses as they appear.

Sterling Connect:Enterprise HTTP Documentation

The Sterling Connect:Enterprise HTTP documentation consists of the following publications:

❖ *IBM Sterling Connect:Enterprise HTTP Installation and Administration Guide*

This document is written for a UNIX or Microsoft Windows administrator responsible for the initial set up of Sterling Connect:Enterprise HTTP. It includes installation and configuration procedures for Sterling Connect:Enterprise HTTP on Microsoft Windows and UNIX operating systems.

❖ Sterling Connect:Enterprise HTTP Help

The Help is written for all users of Sterling Connect:Enterprise HTTP. It includes information on sending and receiving text or binary data between a local system and a Sterling Connect:Enterprise data repository. The Help system also contains an explanation and a course of action for all error messages. You can access the Help from the Sterling Connect:Enterprise HTTP Main page.

❖ *IBM Sterling Connect:Enterprise HTTP Release Notes*

This document is written for a UNIX or Microsoft Windows administrator responsible for the initial set up of Sterling Connect:Enterprise HTTP. It describes features and last-minute product information.

About Sterling Connect:Enterprise HTTP

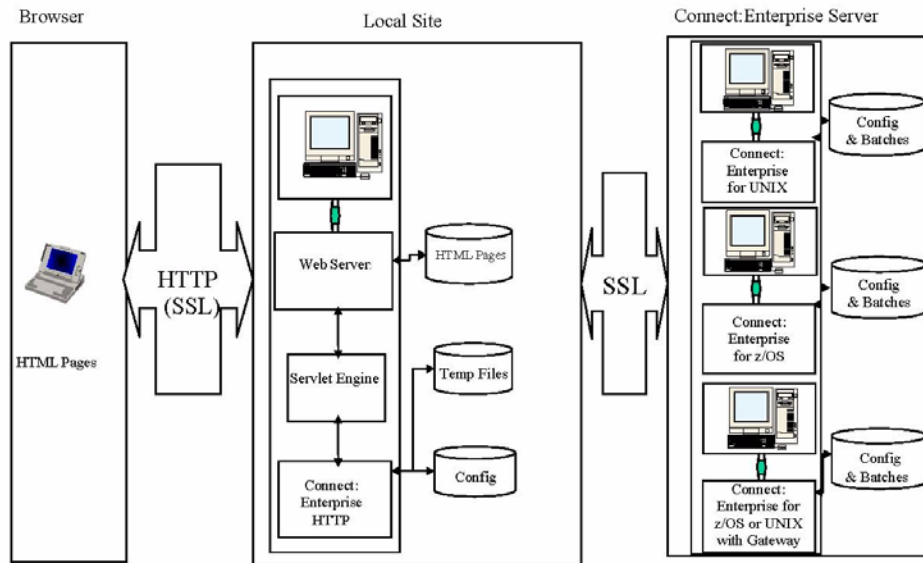
Sterling Connect:Enterprise HTTP is a Web-based utility that enables users to communicate with the Sterling Connect:Enterprise data repository through the Internet. Supported Sterling Connect:Enterprise data repositories are:

- ❖ IBM Sterling Connect:Enterprise for UNIX
- ❖ IBM Sterling Connect:Enterprise for z/OS®
- ❖ IBM Sterling Connect:Enterprise for z/OS with IBM Sterling Connect:Enterprise Gateway

The Sterling Connect:Enterprise HTTP software resides on a Web server and is supported by a servlet engine, which also resides on the Web server.

As a Web-based utility, Sterling Connect:Enterprise HTTP enables you to request, distribute, and track data on the Sterling Connect:Enterprise data repository from any location, requiring only a Web browser and a link to the Internet or an intranet.

From a Sterling Connect:Enterprise HTTP HTML page, you submit a request. The HTML page contains attributes that identify the operation you are performing. Property files contain the parameters that are not specified in the HTML page attributes. Sterling Connect:Enterprise HTTP uses the attributes and the property files to formulate a request to the servlet engine. The servlet engine sends the request to Sterling Connect:Enterprise over an FTP connection. Sterling Connect:Enterprise processes the request and returns it to Sterling Connect:Enterprise HTTP and Sterling Connect:Enterprise HTTP converts it to HTML. You can view the response to your request with your Web browser. The following diagram illustrates the relationship between Sterling Connect:Enterprise HTTP and the Sterling Connect:Enterprise server:



Sterling Connect:Enterprise HTTP Functions

Sterling Connect:Enterprise HTTP enables users to:

- ❖ Log on to a Sterling Connect:Enterprise server.
- ❖ Send text or binary data from their local system to a Sterling Connect:Enterprise server.
- ❖ Receive text or binary data from a Sterling Connect:Enterprise server on their local system.
- ❖ Limit access to Sterling Connect:Enterprise HTTP and the Sterling Connect:Enterprise server.
- ❖ Protect the information sent and received using Sterling Connect:Enterprise HTTP.

Installing Sterling Connect:Enterprise HTTP

This chapter describes the procedures for upgrading and installing Sterling Connect:Enterprise HTTP on the UNIX operating system and the Microsoft Windows operating systems. This chapter also contains instructions for uninstalling the product.

Before You Begin

Before you begin the installation, complete the following tasks:

- ❖ Review the *IBM Sterling Connect:Enterprise HTTP Release Notes* for any changes in the product or installation procedure. It contains the latest product information. The information in this document may affect your installation procedures and definitions.
- ❖ Verify that your system meets product hardware and software requirements. Refer to the *IBM Sterling Connect:Enterprise HTTP Release Notes* for specific requirements and recommendations.
- ❖ These installation procedures assume that all other Sterling Connect:Enterprise components and third-party applications are installed and ready for use. These components include Sterling Connect:Enterprise TCP/IP, FTP, SNA network, and database connectivity. Refer to the *IBM Sterling Connect:Enterprise HTTP Release Notes* for the specific system requirements.
- ❖ Verify that you have installed and configured your Web server and servlet engine and that they are communicating with each other. This is required before you can configure Sterling Connect:Enterprise HTTP.
- ❖ If you are upgrading from a previous release of Sterling Connect:Enterprise HTTP, perform the procedure *Upgrading Sterling Connect:Enterprise HTTP on the UNIX OS* on page 14 or *Upgrading Sterling Connect:Enterprise HTTP on Microsoft Windows* on page 16.

Installing Sterling Connect:Enterprise HTTP on the UNIX OS

The following procedure installs Sterling Connect:Enterprise HTTP on a UNIX workstation. Install Sterling Connect:Enterprise HTTP using the same user ID that was used to install the Web server and servlet engine. Using the same ID avoids any file permission problems.

Note: In the installation script, the defaults are in upper-case letters and contained in brackets ([]). To accept the default, press **Enter**. Also, on questions that do not require a Y|N answer, type a question mark (?) to view a more detailed explanation.

To install Sterling Connect:Enterprise HTTP, follow these steps:

1. From your installation media, type `./CEHTTP.Vxx.platform.bin` and press **Enter**.
2. At the **Introduction** prompt, press **Enter**.
3. At the **Choose Installation Folder** prompt, type `y` to accept the default or `n` to specify a different directory and press **Enter**.
4. At the **Sterling Connect:Enterprise Servlet Info** prompt, specify the servlet that will handle requests and press **Enter**.
5. At the **Session Timeout Value** prompt, type the session timeout value and press **Enter**. This value specifies the number of seconds of idle time users have before they are automatically logged off the Sterling Connect:Enterprise server. The default is 300 seconds. The maximum is 1800 seconds.
6. At the **Sterling Connect:Enterprise Server Property File** prompt, type the logical name of the server that Sterling Connect:Enterprise HTTP will access and press **Enter**.

You can configure additional Sterling Connect:Enterprise servers after the installation procedure is complete. You must create a server property file for each Sterling Connect:Enterprise server accessed by Sterling Connect:Enterprise HTTP. See Chapter 5, *Customizing Property Files*, for more information about the server property file and about setting up additional Sterling Connect:Enterprise servers.

7. At the **Sterling Connect:Enterprise Server** prompt, type the IP address or fully qualified host name of the default Sterling Connect:Enterprise server and press **Enter**.
8. At the **Sterling Connect:Enterprise Server Port** prompt, type the FTP port number for the default Sterling Connect:Enterprise server and press **Enter**.
9. At the **Pre-installation Summary** prompt, review the information for accuracy and press **Enter**.

You must configure the servlet engine before using Sterling Connect:Enterprise HTTP. Refer to Chapter 3, *Configuring the Servlet Engine*, for detailed instructions.

Upgrading Sterling Connect:Enterprise HTTP on the UNIX OS

This procedure protects your current property files from being overwritten. Use this procedure if you are upgrading from a previous version of Sterling Connect:Enterprise HTTP.

This procedure installs Sterling Connect:Enterprise HTTP on a UNIX workstation. Install Sterling Connect:Enterprise HTTP using the same user ID that was used to install the Web server and servlet engine. Using the same ID avoids any file permission problems.

Note: Note: Do not attempt to upgrade a deployed cehttp.war file on the web server. You must install/upgrade to a separate directory and then redeploy the war file.

Note: In the installation script, the defaults are in upper-case letters and contained in brackets ([]). To accept the default, press **Enter**. Also, on questions that do not require a Y|N answer, type a question mark (?) to view a more detailed explanation.

1. Go to the location in web server where cehttp.war was deployed and copy the properties directory to a safe location.
2. At the **Introduction** prompt, press **Enter**.
3. At the **Choose Installation Folder** prompt, specify the existing installation folder and press **Enter**.
4. At the **IBM Sterling Connect:Enterprise Installation Detected** prompt, select **Upgrade Existing Installation** and press **Enter**.
5. At the **Pre-Installation Summary** prompt, review the information for accuracy and press **Enter**.
6. Remove the cehttp application from the web server and redeploy the upgraded cehttp.war.
7. Replace the property folder on the web server with previously saved property folder.

You must configure the servlet engine before using Sterling Connect:Enterprise HTTP. Refer to Chapter 3, *Configuring the Servlet Engine* for detailed instructions.

Installing Sterling Connect:Enterprise HTTP on Microsoft Windows

Use this procedure to install Sterling Connect:Enterprise HTTP for the first time. The installation application displays default values in dialog boxes where applicable.

1. From the installation media, double-click **CEHTTP.Vxx.Win.exe**.
2. On the **Introduction** dialog box, click **Next**.
3. In the **Choose Installation Folder** dialog box, specify the installation folder and click **Install**.
4. In the **Sterling Connect:Enterprise Servlet Info** dialog box, specify the servlet that will handle requests and click **Next**.
5. In the **Session Timeout Value** dialog box, type the session timeout value and click **Next**. This value specifies the number of seconds of idle time users have before they are automatically logged off the Sterling Connect:Enterprise server. The default is 300 seconds. The maximum is 1800 seconds.
6. In the **Sterling Connect:Enterprise Server Property File** dialog box, type the logical name of the server that Sterling Connect:Enterprise HTTP will access and click **Next**.

You can configure additional Sterling Connect:Enterprise servers after the installation procedure is complete. You must create a server property file for each Sterling Connect:Enterprise server accessed by Sterling Connect:Enterprise HTTP. See Chapter 5, *Customizing Property Files*, for more information about the server property file and about setting up additional Sterling Connect:Enterprise servers.

7. In the **Sterling Connect:Enterprise Server** dialog box, type the IP address or fully qualified hostname of the default Sterling Connect:Enterprise server and click **Next**.

8. In the **Sterling Connect:Enterprise Server Port** dialog box, type the FTP port number for the default Sterling Connect:Enterprise server and click **Next**.
9. On the **Pre-Installation Summary** dialog box, click **Install**.

You must configure the servlet engine before using Sterling Connect:Enterprise HTTP. Refer to Chapter 3, *Configuring the Servlet Engine* for detailed instructions.

Upgrading Sterling Connect:Enterprise HTTP on Microsoft Windows

This procedure protects your current property files from being overwritten. Use this procedure if you are upgrading from a previous version of Sterling Connect:Enterprise HTTP. The installation application displays default values in dialog boxes where applicable.

Note: Note: Do not attempt to upgrade a deployed cehttp.war file on the web server. You must install/upgrade to a separate directory and then redeploy the war file.

1. Go to the location in web server where cehttp.war was deployed and copy the properties directory to a safe location.
2. From the installation media, double-click **CEHTTP.Vxx.Win.exe**.
3. On the **Introduction** dialog box, click **Next**.
4. In the **Choose Installation Folder** dialog box, specify the existing installation folder and click **Install**. If the installation folder you specified is the same folder where the product is already installed, the **IBM Sterling Connect:Enterprise HTTP Installation Detected** screen is displayed. Click **Next** to upgrade.
5. At the **Pre-Installation Summary** prompt, review the information for accuracy and click **Install**.
6. Remove the cehttp application from the web server and redeploy the upgraded cehttp.war.
7. Replace the property folder on the web server with previously saved property folder.

You must configure the servlet engine before using Sterling Connect:Enterprise HTTP. Refer to Chapter 3, *Configuring the Servlet Engine*, for detailed instructions.

Uninstalling Sterling Connect:Enterprise HTTP from a Tomcat Web Server

To Uninstall Sterling Connect:Enterprise HTTP from a Tomcat deployment:

1. Stop your web server.
2. Navigate to the directory where Sterling Connect:Enterprise HTTP is deployed.
3. Remove the cehttp folder and the cehttp.war file.

Uninstalling Sterling Connect:Enterprise HTTP from a SunOne Web Server

1. Copy your property files to a location outside of the cehttp directory to prevent them from being overwritten.
2. Click the **Servers** tab.
3. Click **Manage Servers** in the left frame.
4. Select the server you want to manage and click **Manage**.
5. Click the **Virtual Server Class** tab.
6. Select the class you want to manage and click **Manage**.
7. Select the virtual server that cehttp is installed on and click **Manage**.
8. Click the **Web Applications** tab.
9. Click **Edit Web Applications**.
10. Select cehttp and in the **Action** field, select **Delete**. Click **OK** on the pop-up dialog box.

Uninstalling Sterling Connect:Enterprise HTTP from IBM Websphere Web Server

1. On the **WebSphere Integrated Solutions Console**, expand **Applications** in the left-hand panel.
2. Expand **Enterprise Applications**.
3. Enable the checkbox next to **cehttp**, select **Uninstall** and click **OK**.
4. Click **Save Directory to Master Configuration**.

Configuring the Servlet Engine

After you install Sterling Connect:Enterprise HTTP, you must configure the servlet engine before processing requests to Sterling Connect:Enterprise HTTP. This chapter contains configuration instructions for the Web servers, and instructions for verifying your configuration.

Note: All back slashes ("\") in path names in this file are forward slashes ("/") in UNIX.

Configuring the Tomcat Servlet Engine for Sterling Connect:Enterprise HTTP

Complete the following steps to configure Tomcat for a new installation on either a UNIX or Microsoft Windows. In this procedure, replace `{TOMCAT_ROOT_DIR}` with the directory where Tomcat is installed.

Before you begin this configuration, ensure that your Tomcat servlet is communicating properly with the Apache Web server. You can do this by testing one of the sample applications provided with Tomcat.

1. Move **cehttp.war** from the directory where Sterling Connect:Enterprise HTTP is installed to the `{TOMCAT_ROOT_DIR}/webapps` directory.
2. Start Tomcat. Tomcat automatically deploys the Sterling Connect:Enterprise HTTP WAR file.
3. Move the system property file (named **system**) from the directory where Sterling Connect:Enterprise HTTP is installed to the following directory:

```
{TOMCAT_ROOT_DIR}\webapps\cehttp\property\
```

4. Move the server property file (named in item 4 on page 70 for UNIX or in item 2 on page 72 for Microsoft Windows) from the directory where Sterling Connect:Enterprise HTTP is installed to the following directory:

```
{TOMCAT_ROOT_DIR}\webapps\cehttp\property\server\
```

5. After the initial startup, use the following URL to run Sterling Connect:Enterprise HTTP. The default port value for Tomcat is 8080. You can omit the port value if you are using port 80.

```
http://servername:port/cehttp/html/main.htm
```

Configuring the Tomcat Servlet Engine to Upgrade Sterling Connect:Enterprise HTTP

Use the following procedure to configure Tomcat for a Sterling Connect:Enterprise HTTP upgrade on either a UNIX or Microsoft Windows. In this procedure, replace `{TOMCAT_ROOT_DIR}` with the directory where Tomcat is installed.

1. Stop Tomcat.
2. Navigate to the following directory:

```
{TOMCAT_ROOT_DIR}\webapps\
```

3. To retain your property files, move them to a directory outside of the cehttp folder.
4. Remove the cehttp folder and the cehttp.war file.
5. Move **cehttp.war** from the directory where Sterling Connect:Enterprise HTTP is installed to the `{TOMCAT_ROOT_DIR}/webapps` directory.
6. Start Tomcat. Tomcat automatically deploys the Sterling Connect:Enterprise HTTP WAR file.
7. Move the property files back into the cehttp directory.
8. After the initial startup, use the following URL to run Sterling Connect:Enterprise HTTP. The default port value for Tomcat is 8080. You can omit the port value if you are using port 80.

```
http://servername:port/cehttp/html/main.htm
```

Configuring the Sun ONE Web Server

Use the following procedure to configure Sun ONE for Sterling Connect:Enterprise HTTP on either a UNIX or Microsoft Windows OS. In this procedure, replace `{Sun ONE_ROOT_DIR}` with the directory where Sun ONE is installed.

1. Start your Sun ONE Web Server.
2. Sign on to the Sun ONE Administration Server using your Sun ONE administrator user name and password.
3. If you are installing Sterling Connect:Enterprise HTTP for the first time, go to step 4. If you are upgrading from a previous version, perform the following:
 - a. Copy your property files to a location outside of the cehttp directory to prevent them from being overwritten.
 - b. Click the **Servers** tab.
 - c. Click **Manage Servers** in the left frame.
 - d. Select the server you want to manage and click **Manage**.
 - e. Click the **Virtual Server Class** tab.
 - f. Select the class you want to manage and click **Manage**.
 - g. Select the virtual server that cehttp is installed on and click **Manage**.
 - h. Click the **Web Applications** tab.

- i. Click **Edit Web Applications**.
 - j. Select cehttp and in the **Action** field, select **Delete**. Click **OK** on the pop-up dialog box.
 - k. At the top of the screen, click the name of the server (the left-most button).
 - l. At the top of the screen, select **Web Server Administration Server**.
4. Click the **Servers** tab.
 5. Click **Manage Servers** in the left frame.
 6. Select the server you want to manage and click **Manage**.
 7. Click the **Virtual Server Class** tab, select the class you want to manage and click **Manage**.
 8. Click **Manage Virtual Servers** in the left frame.
 9. Select the correct Virtual Server and click **Manage**.
 10. Click the **Web Applications** tab.
 11. Click **Deploy Web Application** in the left frame.
 12. Type the following information and click **OK**.

Field	Information
WAR File On	The machine where the WAR file is located (local or server)
WAR File Path	Path and file name of the cehttp.war file. For example: C:\CEHTTP Option\cehttp.war
Application URL	/cehttp
Installation Directory	Accept the default

13. Click **OK** when the *Web Application successfully deployed* message is displayed.

You may get the following message:

Bad Request
Your browser sent a query this server could not understand.

This is normal and does not affect the servlet configuration.

14. Click **Apply**.
15. Close the Web Server Administration Server.
16. If this is a new install, copy the system property file to the property directory where cehttp is deployed. If you are upgrading, copy your property files from the directory where Sterling Connect:Enterprise HTTP is installed to the property directory where cehttp is deployed.
17. Use the following URL to run Sterling Connect:Enterprise HTTP. You can omit the port value if you are using port 80.

`http://servername:port/cehttp/html/main.htm`

Configuring the IBM WebSphere Web Server

Use the following procedure to configure WebSphere for Sterling Connect:Enterprise HTTP on the Microsoft Windows or UNIX OS. In this procedure, replace {*WebSphere_ROOT_DIR*} with the directory where WebSphere is installed.

Before you begin this configuration, ensure that your WebSphere servlet is communicating properly with the IBM HTTP server.

1. If you are installing Sterling Connect:Enterprise HTTP for the first time, go to step 2 on page 22. If you are upgrading Sterling Connect:Enterprise HTTP, do the following:
 - a. Copy the property files you want to retain to a location outside of the cehttp directory.
 - b. On the **WebSphere Integrated Solutions Console**, expand **Applications** in the left-hand panel.
 - c. Expand **Enterprise Applications**.
 - d. Enable the checkbox next to **cehttp**, select **Uninstall** and click **OK**.
 - e. Click **Save Directory to Master Configuration**.
2. On the **WebSphere Integrated Solutions Console**, expand **Applications** in the left-hand panel.
3. Click **Enterprise Applications** and select **Install**.
4. Specify the following parameters, and click **Next**.

Parameter	Value
Path	Path and file name of the cehttp.war file. For example: C:\CEHTTP Option\cehttp.war
Context Root	/cehttp

5. Accept the defaults on the remaining screens until you are finished.
It can take several minutes to deploy Sterling Connect:Enterprise HTTP.
6. Click **Save Directory to Master Configuration**.
7. Expand **Enterprise Applications**.
8. Enable the checkbox next to **cehttp.war**, and click **Start**.
9. If this is a new install, copy the system property file to the property directory where cehttp is deployed. If this is an upgrade, move the property files you retained back into the cehttp directory.
10. Use the following URL to run Sterling Connect:Enterprise HTTP. You can omit the port value if you are using port 80.

`http://servername:port/cehttp/html/main.htm`

Configuring Security

Sterling Connect:Enterprise HTTP offers two types of security: user and data. User security limits who has access to Sterling Connect:Enterprise HTTP and the Sterling Connect:Enterprise server. Data security protects the information sent and received using Sterling Connect:Enterprise HTTP.

User Security

Sterling Connect:Enterprise HTTP secures the link between Sterling Connect:Enterprise HTTP and Sterling Connect:Enterprise servers by allowing only authorized users to get into, but not past, the repository. This method ensures the security of the system and the data. To access Sterling Connect:Enterprise HTTP, users must have a Sterling Connect:Enterprise user ID and password. Without a user ID and password, users can view the HTML pages, but cannot make requests of the Sterling Connect:Enterprise data repository.

Sterling Connect:Enterprise HTTP enables administrators to specify various initialization parameters and property keys that limit the Sterling Connect:Enterprise servers with which users interact. The Sterling Connect:Enterprise server provides the security, but you can prevent requests from being sent to a server by not defining those servers in either the server property files or the system property file.

Data Security

Another level of security is the one between the Web browser and the Web server. This security is not provided by Sterling Connect:Enterprise HTTP. However, Sterling Connect:Enterprise HTTP does support the Secure Sockets Layer (SSL) protocol, a protocol that provides secure communications with transport protocols, including FTP over TCP/IP. It is an open, nonproprietary Internet protocol that is widely adopted as standard.

When using the SSL protocol, Sterling Connect:Enterprise HTTP ensures point-to-point security, meaning that the data is secured as it is transmitted across a single socket. To use the SSL protocol with Sterling Connect:Enterprise HTTP, the Sterling Connect:Enterprise server you communicate with must have Secure FTP functionality. You must also configure the Sterling Connect:Enterprise HTTP SSL property files. Refer to *Configuring the SSL Property Files* on page 28 for more information on configuring the property files for the SSL protocol.

Cryptography

Cryptography involves algorithms that transform a readable text message into an encrypted text (called cipher text). There are two categories of cryptographic algorithms, symmetric and public key (asymmetric).

Symmetric cryptography requires the sender and receiver to share one key. The key is used to both encrypt and decrypt the data. Public key cryptography requires a private key, known only by the owner, and a public key, which can be disseminated freely. Data encrypted with the private key can only be decrypted with the public key, and vice versa. Symmetric algorithms are much faster than public key algorithms, but require securely transmitting the key to trusted partners.

Authentication

A message digest algorithm, also called a one-way hash function, is used to create a hash (a short, fixed-length representation of a longer, variable-length plain text message). The resulting value of the hash cannot be used to derive the original message. The hash is also called a digest.

When a message digest is encrypted with a private key, the result is a digital signature. Digital signatures allow a client to authenticate the server, because the client has the public key of the server and can use it to decrypt the signature (created with the private key). The client knows the server is the only one who has the private key, so the server must be the one that sent the message.

Clients and servers obtain public keys as part of a certificate that is signed by a trusted, well-known entity called a certificate authority (CA). CAs are responsible for verifying and processing certificate requests, and issuing and managing certificates.

Certificates typically contain:

- ❖ Distinguished name and public key of the server or client
- ❖ Distinguished name and digital signature of the CA
- ❖ Period of validity (certificates expire and must renewed)
- ❖ Administrative and extended information

You obtain a certificate from a CA by first generating a certificate signing request (CSR) that contains specific information in a specific format about the requester. The CA analyzes those fields in the CSR, validates the accuracy of those fields, generates a certificate, and sends it to the requester.

Client-Server Session

Sterling Connect:Enterprise HTTP makes use of both symmetric and asymmetric key algorithms. A client-server session begins with a handshake sequence in which the following actions occur:

- ❖ The client obtains the public key of the server using certificates.
- ❖ The client generates a symmetric session key and sends a message to the server, encrypted with the public key of the server, which contains the session key.
- ❖ The server decrypts this message with its private key to obtain the session key.
- ❖ The client and server use the session key to encrypt and decrypt the rest of the transmitted data.

The server does not need any information about the client, and the client needs to know only the public key of server. The private key of the server is kept secret and is never transmitted. The bulk of the communication is secured with relatively speedy symmetric key algorithms.

Obtaining a Certificate

The first step to using secure communication is to generate a public/private key pair and a CSR. The key pair and CSR are generated using IBM® Sterling Certificate Wizard, which is shipped with Sterling Connect:Enterprise HTTP. Refer to Sterling Certificate Wizard Help for specific instructions. After the CSR has been generated, you must send it to the CA of your choice. This is done either online or by e-mail. After the CA has verified the information in the CSR, you receive a certificate file. As soon as you receive the certificate file, make a backup copy of your certificate. Certificates can become corrupted or can be accidentally deleted. If you lose your certificate and do not have a backup, you must acquire a new certificate.

Note: If you paste your CSR information into a text file, ensure that there are no leading spaces.

Creating the Key Certificate File

The certificate you received from the CA is used to create the key certificate file. This file is a combination of your certificate and the private key you created with Sterling Certificate Wizard.

Complete the following steps to create the key certificate file.

1. Make a backup copy of your certificate if you have not already done so.
2. Install the CA trusted root certificate.

You must obtain a trusted root certificate from the CA or from the system administrator of the Sterling Connect:Enterprise site with which you communicate. You must create a trusted root certificate file (for example, *trusted.txt*) and add your CA trusted root certificate to the file. Each trusted root certificate must be in X.509, BER-encoded PEM format. Your trusted root certificate file should not contain more than one certificate for each CA. Superseded or expired root certificates should be removed.

3. Create your key certificate file.

The key certificate file is created by concatenating your certificate to your private key. The key certificate file name and location can be specified as needed.

For UNIX, you can use the following command:

```
cat privkey.txt cert.txt > keycert.txt
```

For Microsoft Windows, create a separate file and copy the contents of your private key file followed by the contents of your certificate.

The private key must be in PKCS#8, BER-encoded base64-encoded format. Sterling Certificate Wizard automatically creates your private key in this format. The certificate must be in X.509, BER-encoded base64-encoded format. If you require more than one certificate, you can create a certificate chain by concatenating each certificate to the end of the key certificate file. The first certificate should be the certificate and each following certificate should be the signer of the certificate immediately preceding it in the chain.

Use Sterling Certificate Wizard to verify your key certificate file.

4. Make a secure backup copy of your key certificate file.

You always want to have a backup copy of your key certificate file. This file can become corrupted or can be accidentally deleted. If you lose your key certificate file and do not have a backup, you must acquire a new certificate. If a third party gains access to your private key, they could access secure data transfers and masquerade as the server.

Protecting Your SSL Passphrase

When the key pair is generated with Sterling Certificate Wizard, a passphrase is used for SSL connections. This passphrase is stored in clear text in the file and in the property files unless you choose to encrypt it.

Complete the following steps to encrypt your SSL passphrase.

1. Create a text file with any name.
2. Type the following command into the text file:

```
ssl_passphrase=passphrase
```

Note: Replace *passphrase* in the command with the passphrase you chose when you created the key pair.

3. From the *cehttp/tools* directory, type the following command:

```
java -classpath pfcheck.jar cepassprotect -f filename
```

Note: Replace *filename* in the command with the name of the file you created in step 1.

The encrypted passphrase is output to the text file in the following format:

```
ssl_passphrase=ENCRYPTED_XXXXXXXXXXXXXXXXXXXXXX
```

4. When you configure your property files for SSL connections, copy this line to the appropriate property file. Refer to Chapter 5, *Customizing Property Files*, for instructions.

Note: You can also use the **cepassprotect** utility to encrypt any passwords in your property files. Simply replace the **ssl_passphrase** key with the **password** key and type the appropriate password.

Customizing Property Files

This chapter provides information about the property files contained within the Sterling Connect:Enterprise HTTP software. It explains the contents of the property files, how to configure your system to use the pfcheck utility to validate customized property files, and how to customize your property files.

How Property Files Work

Sterling Connect:Enterprise HTTP uses property files to determine which servers to connect to, and to specify how to control the look of Web pages used by the system. Property files consist of key/value pairs. The keys represent individual properties. Each key is defined by a value.

Sterling Connect:Enterprise HTTP uses four types of property files: system, server, remote, and directory. Each property file contains information on how the system responds to a request. Depending on how the request is made, the system may reference any one of these property files for instructions on how to proceed.

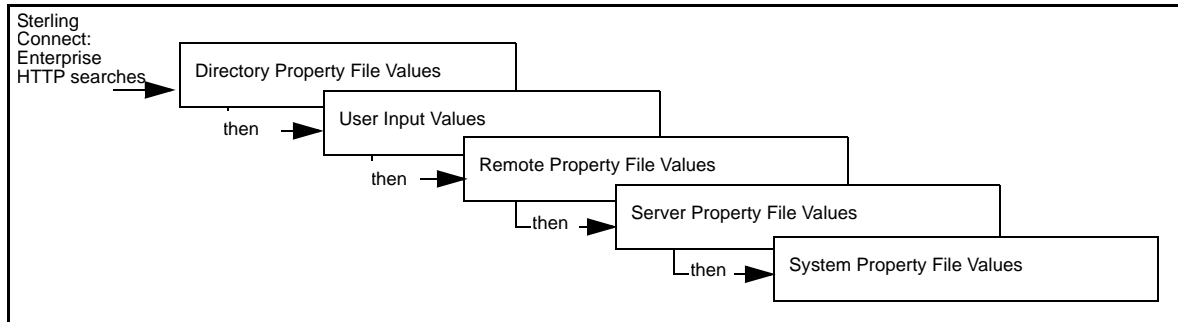
During initialization, Sterling Connect:Enterprise HTTP reads the contents of the system property file and uses the values specified to handle all requests it receives from users. It is often necessary for Sterling Connect:Enterprise HTTP to then reference key values in the remote, server, and directory property files in order to complete a user request.

Priority order for key values is as follows:

1. Directory property file values
2. User-specified property file values
3. Remote property file values
4. Server property file values
5. System property file values

Sterling Connect:Enterprise HTTP first searches for key values in the directory property file, then searches user input. If no key values are specified in the user input, Sterling Connect:Enterprise HTTP searches the remote, server, and system property files (in priority order) to get the necessary information.

The following diagram illustrates this hierarchy.



The pfcheck Utility

Sterling Connect:Enterprise HTTP comes with a utility that checks the syntax of keys and values to verify that you have typed them correctly. The syntax utility is called `pfcheck`. It is a stand-alone application that performs syntax checks on all customized Sterling Connect:Enterprise HTTP property files. It verifies the keywords and their corresponding values in the property files. If `pfcheck` finds any discrepancies, it notifies you by displaying the findings on the screen. The procedure for running `pfcheck` is included in each procedure for customizing the property files.

Configuring the SSL Property Files

You must make specific changes to the property files to enable security at the system, server, or remote level. Place security-related keywords in the system property file to implement security at the system level, in the server property file to implement security at the server level, or in the remote property file to implement security at the remote level. In order for security to function, the keywords can only be added to one file, not spread out over all three. The security keywords are **`cipher_strength`**, **`keycert_file`**, **`root_cert_file`**, **`security_policy`**, **`ssl_client_ccc`**, and **`ssl_passphrase`**.

Refer to *Customizing the System Property File* on page 29 for information on updating the security-related keywords.

Customizing the System Property File

The system property file contains all key values and defaults used by Sterling Connect:Enterprise HTTP for requests. After Sterling Connect:Enterprise HTTP is initialized, the system reads the system property file and provides the software with the necessary values to handle user requests. Unless you plan to change the keys of the Sterling Connect:Enterprise HTTP property files, it is not necessary to customize them. Following is a sample system property file.

```
#
#           System Property File
#
# This file serves as the sample file for system property file.
#
# Not all fields are required. If a certain property is to be used,
# remove the # sign for that property line and assign the proper value.
#
# -----
#servlet_info=IBM Sterling CONNECT:Enterprise HTTP
#defined_remotes_only=N
#remote=default_remote_property_file_name
#mailbox_server=default_server_property_file_name
#directory=default_directory_property_file_name
#mailbox_id=default_mailboxid
#directory_in_memory=N
#data_format=B
#session_timeout=300
#
# -----
# SSL security policy. If security_policy=Y, other parms are allowed.
# root_cert_file and keycert_file are filenames in the server directory.
#
#security_policy=N
#root_cert_file=trusted_root_certificate_file
#cipher_strength=all
#keycert_file=key_certificate_file
#ssl_passphrase=ENCRYPTED_passphrase_for_keycert_private_key
```

Use the following procedure to customize the system property file. In this procedure, replace *Installation_Directory* with the directory where you installed Sterling Connect:Enterprise HTTP.

1. Navigate to the following directory:

```
Installation_Directory\cehttp\property
```

2. Open the file named **system** with any plain-text editor such as Notepad, WordPad, or vi editor.
3. Based on the definitions and valid values in *System Property File Key/Value Pairs* on page 30, modify the Key/Value pairs. You can add a key, remove a key, or change a key value.

Note: Keys are case sensitive. If the keys are not specified correctly, Sterling Connect:Enterprise HTTP ignores them and uses default keys and values.

4. Save the property file.
5. Validate your changes with the pfcheck utility using the following command:

```
java -classpath CEHTTP_Deploy_Directory/cehttp/tools/pfcheck.jar pfcheck -system
system
```

The following table describes the parameters for pfcheck:

Argument	Definition
<i>CEHTTP_Deploy_Directory</i>	Directory inside your Web server directory where Sterling Connect:Enterprise HTTP is deployed.

For help with the pfcheck utility, type **java pfcheck -help** or **java pfcheck -?**

- Restart the servlet engine.

System Property File Key/Value Pairs

The system property file contains the following keys and possible values:

Key	Valid Values	Definition
cipher_strength	strong weak <u>all</u>	Specifies the type of cipher suites: strong allows only allows suites greater than 40-bit, weak allows only 40-bit, and all allows both. Strong cipher suites are: <ul style="list-style-type: none"> • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_DES_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Weak cipher suites are: <ul style="list-style-type: none"> • SSL_RSA_EXPORT_WITH_RC4_40_MD5 • SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5 • SSL_RSA_EXPORT_WITH_DES40_CBC_SHA <p>Note: If you specify this key in the system property file, do not specify any security-related keys in the server or remote property files.</p>
data_format	A <u>B</u>	Specifies the data format used for files sent if unspecified. A= ASCII; B=binary. Binary is the default.
defined_remotes_only	Y <u>N</u>	Specifies whether all users have access to the Sterling Connect:Enterprise HTTP software or only those users who are defined in a remote property file. Y means only those users who specify defined remote property files can access the Sterling Connect:Enterprise HTTP software. If the value is Y, at least one remote property file must exist. N means that you do not need to define and reference a remote property file to use the software.
directory	File name	Specifies the directory property file name to use when setting values for directory requests when one is not specified.

Key	Valid Values	Definition
directory_in_memory	Y <u>N</u>	<p>During directory operation in Sterling Connect:Enterprise HTTP, directory information received from Sterling Connect:Enterprise servers is spooled for further processing by Sterling Connect:Enterprise HTTP. This requires write permissions for Sterling Connect:Enterprise HTTP in order to build the temporary file. On some UNIX systems, Sterling Connect:Enterprise HTTP does not have the appropriate write permissions on the file system, which leads to a failure of the directory operation.</p> <p>To avoid this problem, specify directory_in_memory=Y. This builds the directory listing in memory. The default is <code>directory_in_memory=N</code>.</p>
keycert_file	File name	<p>Specifies the fully qualified file name of the key certificate file. When specifying the path, you must use forward slashes (/) for UNIX and double back slashes (\\) for Microsoft Windows NT/2000/XP.</p> <p>Note: If you specify this key in the system property file, you cannot specify any security-related keys in the server or remote property files.</p>
mailbox_id	Remote user ID	<p>Specifies the name of the mailbox ID to use if one is not specified. If no <code>mailbox_id</code> property is specified, the system uses the same user ID value that connects to the Sterling Connect:Enterprise server.</p>
mailbox_server	File name	<p>Specifies the logical name of the Sterling Connect:Enterprise server you are connecting to if one is unspecified. The value for this property must coincide with the name of one of the server property files. You <i>must</i> specify this property or the servlet cannot start.</p>
remote	File name	<p>Specifies the remote property file name or Sterling Connect:Enterprise user ID to use if one is not specified in a request.</p>
root_cert_file	File name	<p>Specifies the fully qualified file name of the trusted root certificate file. When specifying the path, you must use forward slashes (/) for UNIX and double back slashes (\\) for Microsoft Windows NT/2000/XP.</p> <p>Note: If you specify this key in the system property file, you cannot specify any security-related keys in the server or remote property files.</p>
security_policy	Y <u>N</u>	<p>Specifies whether secure SSL connections are required. If security_policy=N is specified, then no attempt is made to establish a secure connection with the Sterling Connect:Enterprise server.</p> <p>If security_policy=Y is specified, then a secure connection is attempted with the Sterling Connect:Enterprise server. If an error occurs, the session fails without attempting a non-secure connection.</p> <p>Note: If you specify this key in the system property file, you cannot specify any security-related keys in the server or remote property files.</p>
servlet_info	String	<p>Specifies the value returned when the <code>getServletInfo()</code> method is invoked.</p>

Key	Valid Values	Definition
session_timeout	nnnn <u>300</u>	<p>Specifies the number of inactive seconds the software waits before the session is terminated. When the time-out period is exceeded, the FTP connection established on behalf of a user between the servlet and a Sterling Connect:Enterprise server is terminated. Units are seconds.</p> <p>The maximum value is 1800.</p> <p>Note: The FTP server time-out, the Web server, or the servlet engine time-outs can override this time-out.</p>
ssl_passphrase	Encrypted passphrase	<p>Specifies the encrypted passphrase used to access the key certificate file. This key and value are created in <i>Protecting Your SSL Passphrase</i> on page 26. Copy and paste the key and value stored in the text file you created.</p> <p>Note: If you specify this key in the system property file, you cannot specify any security-related keys in the server or remote property files.</p>

Customizing the Server Property Files

The server property files contain details on the Sterling Connect:Enterprise servers that process user requests. Users can only make requests of Sterling Connect:Enterprise servers that have an associated server property file. Therefore, you must create a server property file for each Sterling Connect:Enterprise server that is accessed by Sterling Connect:Enterprise HTTP.

The Sterling Connect:Enterprise logical server names are used as the name of the server property files. For example, if you have three Sterling Connect:Enterprise servers called MServer1, MServer 2, and MServer 3 then you can have as many as three server property files named *MServer1*, *MServer2*, and, *MServer3*.

These names are aliases. The alias points to a file that contains the true identity and port number of the Sterling Connect:Enterprise server. For example, if you do not want users to know what the true name of the Sterling Connect:Enterprise server (such as *enterprise.secure.company.com*), you can give the file an alias, such as

company. When users want to receive files from the Sterling Connect:Enterprise server, they type *company* in the **Sterling Connect:Enterprise Server Input** field. Following is a sample server property file:

```
#
#           Server Property File
#
# This file serves as the sample file for server property file.
#
# Not all fields are required. If a certain property is to be used,
# remove the # sign for that property line and assign the proper value.
#
#
# -----
# Address and port number of the Connect:Enterprise FTP server.
# Address may be of the form www.companyname.com or 111.222.33.44.
#
#address=111.111.111.111
#port=10021
#port_range=r0,r1,r2,r3,r4
#port_retry_wait_time=30
#port_retries=0
#ftp_passive_mode=N
#description=IBM Sterling CONNECT:Enterprise HTTP
#directory=directory_property_filename_for_this_server
#trigger_flag=N
#
# -----
# SSL security policy. If security_policy=Y, other parms are allowed.
# root_cert_file and keycert_file are filenames in the server directory.
#
#security_policy=N
#root_cert_file=trusted_root_certificate_file
#cipher_strength=weak
#ssl_client_ccc_policy=DISALLOWED
#keycert_file=key_certificate_file
#ssl_passphrase=ENCRYPTED_passphrase_for_keycert_private_key
#
# -----
# Multiple Download Option - Allows multiple files to be zipped up and
# downloaded together.
# If multiple_download=Y, the Download Confirm and Download Status options
# are turned off.
# Uncomment multiple_download and set to Y to allow downloading multiple
# files into a zip file. The default is N. If set to Y, download_confirm_mode
# is turned off.
# If multiple_download=Y, the zip_entry_format determines how to format
# duplicate filenames
#   zip_entry_format=dir - (default) use batch# as directory
#                       (e.g. 0000070/filename.txt);
#   zip_entry_format=prefix - prepend the batch# to the filename
#                       (e.g. 0000070.filename.txt);
#
#multiple_download=N
#zip_entry_format=dir|prefix
#
# -----
# Download Confirm Option - Require the user to confirm they have saved
# the downloaded file before marking it T for transmitted.
# Only allowed if Multiple Download option is OFF.
#
#download_confirm_mode=N
#
# -----
# Download Status Option - Opens separate status box at download time
# to monitor the status of the download.
# Only allowed if Multiple Download AND Download Confirm are OFF.
# The enable_download_status_file_size value only enables the pop-up
# window for files greater than the given file size, in bytes.
# Default is 0 for all files.
#
#download_status=N
#enable_download_status_file_size=50000000
```

Use the following procedure to customize the server property file:

1. Navigate to the following directory:

```
Installation_Directory\cehttp\property
```

Replace *Installation_Directory* with the Sterling Connect:Enterprise HTTP installation directory.

2. Open the server property file with any plain-text editor such as Notepad, WordPad, or vi editor.
3. Based on the definitions and valid values in *System Property File Key/Value Pairs* on page 30, modify the Key/Value pair.

Note: Keys are case sensitive. If the keys are not specified correctly, Sterling Connect:Enterprise HTTP ignores them and uses default keys and values.

4. Save the property file.
5. Validate your changes with the pfcheck utility using the following command:

```
java -classpath CEHTTP_Deploy_Directory/cehttp/tools/pfcheck.jar pfcheck -server
filename
```

The following table describes the parameters for pfcheck:

Argument	Definition
<i>CEHTTP_Deploy_Directory</i>	Directory inside your Web server directory where Sterling Connect:Enterprise HTTP is deployed.
<i>filename</i>	Name of the server file you are checking. Use the absolute path or relative path of the file.

For help with the pfcheck utility, type **java pfcheck -help** or **java pfcheck -?**

Server Property File Key/Value Pairs

The server property file contains the following keys and possible values:

Key	Valid Values	Definition
address	IP address or domain name (Required)	Specifies either the domain name or IP address (in dotted-decimal notation)

Key	Valid Values	Definition
cipher_strength	strong weak <u>all</u>	<p>Specifies the type of cipher suites: strong allows only cipher suites greater than 40-bit, weak allows only 40-bit, and all allows both.</p> <p>Strong cipher suites are:</p> <ul style="list-style-type: none"> • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_DES_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA <p>Weak cipher suites are:</p> <ul style="list-style-type: none"> • SSL_RSA_EXPORT_WITH_RC4_40_MD5 • SSL_RSA_EXPORT_WITH_DES40_CBC_SHA <p>Note: If you specify this key in the system property file, do not specify any security-related keys in the server or remote property files.</p>
description	User-defined	Specifies descriptive information about this server property file.
directory	User-defined	Specifies a filename in the ./cehttp/property/directory directory which containing directives on which fields to include when displaying the directory page.
download_confirm_mode	Y <u>N</u>	<p>Indicates whether to enable file transfer acknowledgement. If download_confirm_mode=Y is set, the Receive Confirmation window is displayed in addition to the File Download dialog box. You must indicate whether or not the file was successfully received by the server. This ensures that the correct batch flags are set in the Sterling Connect:Enterprise server in the case of a transmission error.</p> <p>Note: If download_confirm_mode=Y is set, some browsers can only receive one file at a time. The Receive function behaves the same as the Directory function.</p>
download_status	Y <u>N</u>	Opens separate status box at download time to monitor the status of the download. Only allowed if Multiple Download AND Download Confirm are OFF. Also works with enable_download_status_file_size.
enable_download_status_file_size	Numeric value	Used with download_status. Enables download status update popup only for files greater than this value. Default is 0 for all files.
ftp_passive_mode	Y <u>N</u>	<p>Specifies whether Sterling Connect:Enterprise HTTP uses normal or passive mode transfer.</p> <p>N specifies normal mode transfer. This is the default.</p> <p>Y specifies passive mode transfer. In this mode, Sterling Connect:Enterprise HTTP sends a PASV command to the Sterling Connect:Enterprise server. The Sterling Connect:Enterprise server returns a valid port and IP address.</p>
keycert_file	File name	<p>Specifies the fully qualified file name of the key certificate file. When specifying the path, you must use forward slashes (/) for UNIX and double back slashes (\\) for Microsoft Windows 2000/NT.</p> <p>Note: If you specify this key in the server property file, you cannot specify any security-related keys in the system or remote property files.</p>

Key	Valid Values	Definition
multiple_download	Y <u>N</u>	<p>Allows multiple files to be zipped up and downloaded together. If multiple_download=Y, the Download Confirm and Download Status options are turned off. Uncomment multiple_download and set to Y to allow downloading multiple files into a zip file. The default is N.</p> <p>If set to Y, download_confirm_mode is turned off. If multiple_download=Y, the zip_entry_format determines how to format duplicate filenames.</p>
port	Port number	Specifies the FTP port number of this Sterling Connect:Enterprise server. If the port number is not specified, it defaults to 10021.
port_range	Port range	<p>Specifies one or more local port ranges used by the data connection when in active mode so they match the range allowed by the firewall. Specify as a comma-separated list. Each range is a hyphen-separated low and high value used to define the port range. You can specify a maximum of 5 port ranges in each server property file. There is no default range.</p> <p>Following is an example: port_range=10022-10200,20022-20022</p>
port_retries	0–99	<p>Specifies the number of times the ports defined in the port_range attribute are re-examined to find an available port.</p> <p>The default value is zero 0, and indicates that port ranges are searched once per socket attempt.</p>
port_retry_wait_time	0–180	<p>Specifies the number of seconds that Sterling Connect:Enterprise HTTP waits before attempting a retry of the port search.</p> <p>The default is 30.</p>
root_cert_file	File name	<p>Specifies the fully qualified file name of the trusted root certificate file. When specifying the path, you must use forward slashes (/) for UNIX and double back slashes (\\) for Microsoft Windows 2000/NT.</p> <p>Note: If you specify this key in the server property file, you cannot specify any security-related keys in the system or remote property files.</p>
security_policy	Y <u>N</u>	<p>Specifies whether secure SSL connections are required. If security_policy=N is specified, then no attempt is made to establish a secure connection with the Sterling Connect:Enterprise server.</p> <p>If security_policy=Y is specified, then a secure connection is attempted with the Sterling Connect:Enterprise server. If an error occurs, the session fails without attempting a non-secure connection.</p> <p>Note: If you specify this key in the system property file, you cannot specify any security-related keys in the server or remote property files.</p>

Key	Valid Values	Definition
ssl_client_ccc_policy	REQUIRED DISALLOWED OPTIONAL	<p>Specifies whether to turn off encryption by issuing an FTP Clear Control Channel (CCC) command in a control socket that has been secured using SSL.</p> <p>DISALLOWED specifies that Sterling Connect:Enterprise HTTP does not issue the FTP CCC command after a secure or unsecured connection has been established with a Sterling Connect:Enterprise server. This is the default.</p> <p>REQUIRED specifies that Sterling Connect:Enterprise HTTP issues an FTP CCC command after it has established a secured connection and the browser user has been authenticated by the Sterling Connect:Enterprise server.</p> <p>OPTIONAL specifies that Sterling Connect:Enterprise HTTP submits an FTP CCC command to the Sterling Connect:Enterprise server. If a positive result code is returned from the server, Sterling Connect:Enterprise HTTP goes into a clear text state for the control socket. If a negative result code is returned from the server, Sterling Connect:Enterprise HTTP stays in an encrypted state.</p>
ssl_passphrase	Encrypted passphrase	<p>Specifies the encrypted passphrase used to access the key certificate file. This key and value are created in <i>Protecting Your SSL Passphrase</i> on page 26. Copy and paste the key and value stored in the text file you created.</p> <p>Note: If you specify this key in the server property file, you cannot specify any security-related keys in the system or remote property files.</p>
trigger_flag	Y N	<p>Indicates if the batch placed in the remote server repository should be immediately sent to other remote sites after an upload operation. If trigger_flag=Y is set in the server or remote property files or the Trigger automatic routing check box is checked on the Upload Web page, then the Sterling Connect:Enterprise server triggers automatic routing.</p> <p>Note: If the action parameters are not specified in the Sterling Connect:Enterprise for UNIX RSD or ACD files, the trigger flag is ignored. If the server is a Sterling Connect:Enterprise for z/OS, the trigger flag is not supported and an error message is generated.</p>
zip_entry_format	dir prefix	<p>If multiple_download=Y, the zip_entry_format determines how to format duplicate filenames:</p> <p>zip_entry_format=dir - (default) use batch# as directory, for example: 0000070/filename.txt.</p> <p>zip_entry_format=prefix - prepend the batch# to the filename, for example: 0000070.filename.txt.</p>

Customizing the Remote Property Files

The remote property files contain values that the Sterling Connect:Enterprise HTTP software uses to process user requests. The actual Sterling Connect:Enterprise user ID and the values used by Sterling Connect:Enterprise HTTP to handle user requests are defined in these files.

Remote property file names are the logical names of the users or groups allowed to use Sterling Connect:Enterprise HTTP. They are set up by the Sterling Connect:Enterprise HTTP administrator. Their names do not have to match the corresponding Sterling Connect:Enterprise user ID, but they can.

Note: If the **defined_remotes_only** key of the system property file is set to **Y**, at least one remote property file must exist.

Following is a sample remote property file:

```
#
#           Remote Property File
#
# This file serves as the sample file for remote property file.
# If defined_remotes_only=Y is set in the system property file, at
# one valid remote property file must exist.
#
# Not all fields are required. If a certain property is to be used,
# remove the # sign for that property line and assign the proper value.
#
# -----
#description=IBM Sterling CONNECT:Enterprise HTTP Test Remote File
#mailbox_server=server_property_file_name
#directory=directory_property_file_name
#user_id=userid
#password=password
#trigger_flag=N
#mailbox_id=mailboxid
#data_format=B
#
# -----
# SSL security policy. If security_policy=Y, other parms are allowed.
# root_cert_file and keycert_file are filenames in the server directory.
#
#security_policy=N
#root_cert_file=trusted_root_certificate_file
#cipher_strength=all
#keycert_file=key_certificate_file
#ssl_passphrase=ENCRYPTED_passphrase_for_keycert_private_key
```

Use the following procedure to customize the remote property file:

1. Navigate to the following directory:

```
Installation_Directory\cehttp\remote\
```

Replace *Installation_Directory* with the Sterling Connect:Enterprise HTTP installation directory.

2. Open the remote property file with any plain-text editor such as Notepad, WordPad, or vi editor.
3. Based on the definitions and valid values in *Remote Property File Key/Value Pairs* on page 40, modify the Key/Value pair.

Note: Keys are case sensitive. If the keys are not specified correctly, Sterling Connect:Enterprise HTTP ignores them and uses default keys and values.

4. Save the property file.
5. Validate your changes with the pfcheck utility using the following command:

```
java -classpath CEHTTP_Deploy_Directory/cehttp/tools/pfcheck.jar pfcheck -remote
filename
```

The following table describes the parameters for pfcheck:

Argument	Definition
<i>CEHTTP_Deploy_Directory</i>	Directory inside your Web server directory where Sterling Connect:Enterprise HTTP is deployed.
<i>filename</i>	Name of the server file you are checking. Use the absolute path or relative path of the file.

For help with the pfcheck utility, type **java pfcheck -help** or **java pfcheck -?**

Remote Property File Key/Value Pairs

The remote property file contains the following keys and possible values:

Key	Valid Values	Definition
cipher_strength	strong weak all	Specifies the type of cipher suites: strong allows only cipher suites greater than 40-bit, weak allows only 40-bit, and all allows both. Strong cipher suites are: <ul style="list-style-type: none"> • SSL_RSA_WITH_RC4_128_MD5 • SSL_RSA_WITH_RC4_128_SHA • SSL_RSA_WITH_DES_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Weak cipher suites are: <ul style="list-style-type: none"> • SSL_RSA_EXPORT_WITH_RC4_40_MD5 • SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5 • SSL_RSA_EXPORT_WITH_DES40_CBC_SHA Note: If you specify this key in the system property file, do not specify any security-related keys in the server or remote property files.
data_format	A <u>B</u>	Specifies the data type used for files sent. A means ASCII and B means binary. Binary is the default.
description	User-defined	Specifies descriptive information about this remote property file.
directory	File name	Specifies the directory property file to use to set values for directory requests.
keycert_file	File name	Specifies the fully qualified file name of the key certificate file. When specifying the path, you must use forward slashes (/) for UNIX and double back slashes (\\) for Microsoft Windows NT/2000/XP. Note: If you specify this key in the remote property file, you cannot specify any security-related keys in the system or server property files.
mailbox_id	User-defined	Specifies the default mailbox ID to use if one is not specified in a request. This parameter is a 1 to 8 character alphanumeric string.

Key	Valid Values	Definition
mailbox_server	File name	Specifies the logical name of the default server to connect with if it is unspecified. This value must coincide with one of the server property file names in the server property file directory. This value is used if no value is specified in the user request.
password	User-defined	<p>Specifies the password corresponding to the user_id property value. If no value is specified, the system assumes that either no password is associated with the user_id or that a password is specified in a request. Password syntax is determined by the Sterling Connect:Enterprise server. Contact your system administrator for information on password syntax.</p> <p>Note: If the password key is assigned to a remote file with password encoding activated, it is not protected by anything other than the operating system file protection. To turn on password encoding, refer to <i>Protecting Your SSL Passphrase</i> on page 26.</p>
root_cert_file	File name	<p>Specifies the fully qualified file name of the trusted root certificate file. When specifying the path, you must use forward slashes (/) for UNIX and double back slashes (\) for Microsoft Windows NT/2000/XP.</p> <p>Note: If you specify this key in the remote property file, you cannot specify any security-related keys in the system or server property files.</p>
security_policy	Y N	<p>Specifies whether secure SSL connections are required. If security_policy=N is specified, then no attempt is made to establish a secure connection with the Sterling Connect:Enterprise server. If security_policy=Y is specified, then a secure connection is attempted with the Sterling Connect:Enterprise server. If an error occurs, the session fails without attempting a non-secure connection.</p> <p>Note: If you specify this key in the system property file, you cannot specify any security-related keys in the server or remote property files.</p>
ssl_passphrase	Encrypted passphrase	<p>Specifies the encrypted passphrase used to access the key certificate file. This key and value is created in <i>Protecting Your SSL Passphrase</i> on page 26. Copy and paste the key and value stored in the text file you created.</p> <p>Note: If you specify this key in the remote property file, you cannot specify any security-related keys in the system or server property files.</p>
trigger_flag	Y N	<p>Indicates if the batch placed in the remote server repository should be immediately sent to other remotes after an upload operation. If trigger_flag=Y is set in the server or remote property files or the Trigger automatic routing check box is checked on the Upload Web page, then the Sterling Connect:Enterprise server triggers automatic routing.</p> <p>Note: If the action parameters are not specified in the Sterling Connect:Enterprise for UNIX RSD or ACD files, the trigger flag is ignored. If the server is a Sterling Connect:Enterprise for z/OS, the trigger flag is not supported and an error message is generated.</p>
user_id	User-defined	Specifies the default user ID used when logging on to the Sterling Connect:Enterprise system if not otherwise specified. If no value is specified for the user_id, then the remote property file name is used if no value is specified in the user request. This value is a 1 to 8 character alphanumeric string.

Customizing the Directory Property Files

The directory property files store content and formatting information used by Sterling Connect:Enterprise HTTP. These files determine the type of data returned in response to a directory request. A system property file, a remote property file, or both, can reference a directory property file. However, it is not necessary to define any directory property files for Sterling Connect:Enterprise HTTP to function.

Following is a sample directory property file:

```
#
#           Directory Property File
#
# This file serves as the sample file for directory property file.
#
# Not all fields are required. If a certain property is to be used,
# remove the # sign for that property line and assign the proper value.
#
# Note: Default values provided except for the description property line.
#
# -----
#description=IBM Sterling CONNECT:Enterprise HTTP Test Directory
#show_batch_id=U
#show_batch_num=Y
#show_creation_date=Y
#show_creation_time=Y
#show_data_format=N
#show_deleted_batches=N
#show_flags=Y
#show_mailbox_id=Y
#show_originator_id=N
#show_size=Y
#show_cezos_record_count=N
#show_cezos_vbqid=N
#show_unrequestable_batches=N
# -----
#
```

Use the following procedure to customize the directory property file:

1. Navigate to the following directory:

```
Installation_Directory\cehttp\property
```

Replace *Installation_Directory* with the Sterling Connect:Enterprise HTTP installation directory.

2. Open the directory property file with any plain-text editor such as Notepad, WordPad or vi editor.
3. Based on the definitions and valid values in *Directory Property File Key/Value Pairs* on page 43, modify the Key/Value pair.

Note: Keys are case sensitive. If the keys are not specified correctly, Sterling Connect:Enterprise HTTP ignores them and uses default keys and values.

4. Save the property file.
5. Validate your changes with the pfcheck utility using the following command:

```
java -classpath CEHTTP_Deploy_Directory/cehttp/tools/pfcheck.jar pfcheck
-directory filename
```

The following table describes the parameters for pfcheck:

Argument	Definition
<i>CEHTTP_Deploy_Directory</i>	Directory inside your Web server directory where Sterling Connect:Enterprise HTTP is deployed.
<i>filename</i>	Name of the server file you are checking. Use the absolute path or relative path of the file.

For help with the pfcheck utility, type **java pfcheck -help** or **java pfcheck -?**

Directory Property File Key/Value Pairs

The directory property file contains the following keys and possible values:

Key	Valid Values	Definition
description	User-defined	Specifies descriptive information about this directory property file.
show_batch_id	Y N <u>U</u>	Indicates whether batch IDs for batches are displayed for directory list operations if unspecified. Y means yes. N means no. U means yes and also that batch IDs are displayed as URLs so that if selected, a receive operation is initiated. The value in the directory is the batch ID. Note: If users of Sterling Connect:Enterprise HTTP are using Internet Explorer for their Web browser, set this key to U . If not, Internet Explorer users cannot receive any files.
show_batch_num	<u>Y</u> N	Indicates whether batch numbers for batches are displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is the batch number.
show_cezos_record_count	Y <u>N</u>	Determines if the directory output contains a column for the Sterling Connect:Enterprise z/OS record count field. The default is No. If not connected to a Sterling Connect:Enterprise z/OS, this parameter has no meaning.
show_cezos_vbqid	Y <u>N</u>	Determines if the directory output contains a column for the Sterling Connect:Enterprise z/OS VBQ id field. The default is No. If not connected to a Sterling Connect:Enterprise z/OS, this parameter has no meaning.
show_creation_date	<u>Y</u> N	Indicates whether the creation dates of batches are displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is the creation date of the batch in MonthDDCCYY format.
show_creation_time	<u>Y</u> N	Indicates whether the creation times of batches are displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is the creation time of the batch in HHMM format.
show_data_format	Y <u>N</u>	Indicates whether the data types of batches are displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is A for ASCII or B for binary. Note: The data format is presented from the perspective of the user not from the Sterling Connect:Enterprise server view.

Key	Valid Values	Definition
show_flags	<u>Y</u> N	Indicates whether the flag values for batches are displayed for directory list operations if unspecified. Y means yes. N means no. The values in the directory are Sterling Connect:Enterprise flags, such as RTME.
show_mailbox_id	<u>Y</u> N	Indicates whether the mailbox IDs for batches are displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is the mailbox ID.
show_originator_id	Y <u>N</u>	Indicates whether the originator of the batch is displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is the name of the remote or user that added the batch.
show_deleted_batches	Y <u>N</u>	Indicates whether the logically deleted batches are displayed for directory list operations if unspecified. Y means yes. N means no.
show_unrequestable_batches	Y <u>N</u>	Indicates whether only the transmittable batches are displayed for directory list operations if unspecified. Y means yes. N means no.
show_size	<u>Y</u> N	Indicates whether the sizes of batches are displayed for directory list operations if unspecified. Y means yes. N means no. The value in the directory is the size of the batch in bytes.

Customizing the User Interface

This chapter provides information on customizing the Sterling Connect:Enterprise HTTP user interface.

Using the Change Password Function

If you are using a Sterling Connect:Enterprise server that supports the change password function, you will need to change the logon page. Perform the following:

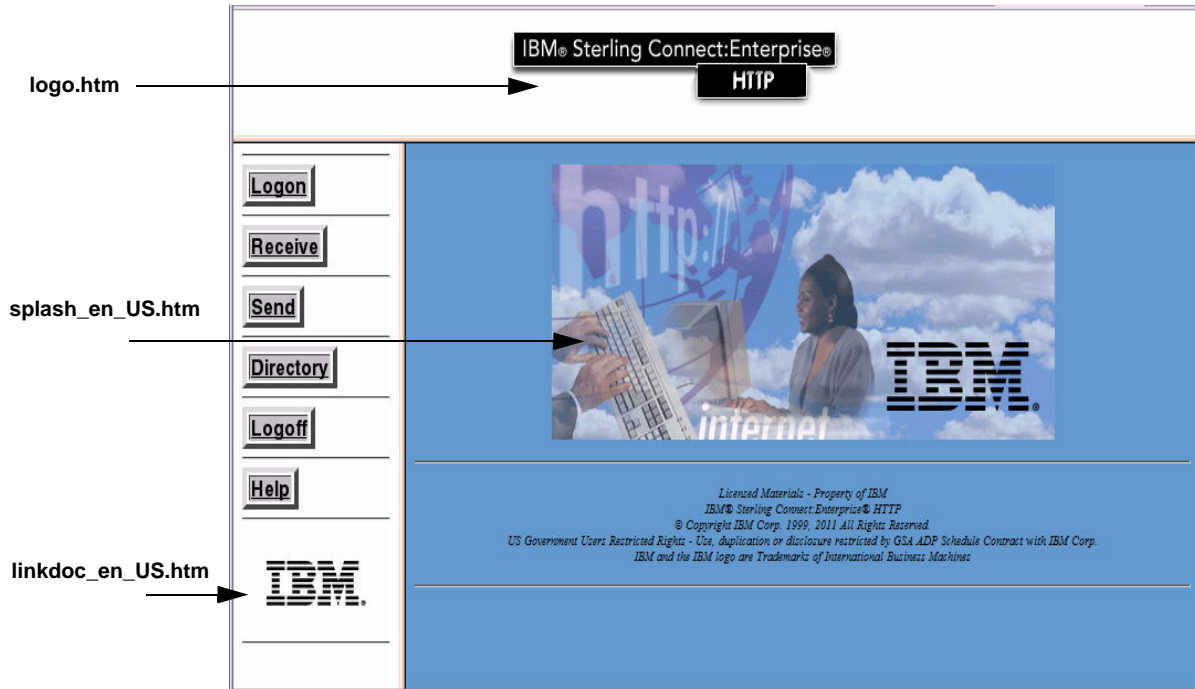
1. In the *Installation_Directory*\cehttp\html folder, rename **logon_en_US.htm** to **logon_en_US.htm.nopassword**
2. In the *Installation_Directory*\cehttp\html folder, rename **logon_en_US.htm.changepassword** to **logon_en_US.htm**

Installation_Directory is the directory where Sterling Connect:Enterprise HTTP is installed.

Customizing Your HTML Pages

You can change the look of the user interface by editing the HTML pages. These pages are located in the *Installation_Directory*\cehttp\html directory. *Installation_Directory* is the directory where Sterling Connect:Enterprise HTTP is installed.

The main page is made up of three different pages displayed in three frames as follows:



You can customize each of these pages to display different graphics. Use the following procedure:

1. Place the graphics you want to use in the *Installation_Directory*\cehttp\html\images directory.
2. Open and edit the HTML page and replace the original graphic name with the name of the graphic you placed in step 1. The following table identifies the original name of the graphic in each page.

Page	Name of the Original Graphic
logo.htm	mbwa.gif
splash_en_US.htm	wasplash.gif
linkdoc_en_US.htm	sterlogo.gif

3. Save the HTML page.

Additionally, you can edit the remaining HTML pages by adding or removing the appropriate HTML code.

Page	HTML File Name	Description
Logon	logon_en_US.htm	Is displayed when you click Logon .
Send	upload_en_US.htm	Is displayed when you click Send .
Receive	download_en_US.htm	Is displayed when you click Receive .
Directory	dirlist_en_US.htm	Is displayed when you click Directory .
Help	help_en_US.htm	Is displayed when you click Help .

Redirecting Sterling Connect:Enterprise HTTP

Sterling Connect:Enterprise HTTP enables you to change the way Sterling Connect:Enterprise HTTP behaves after an event. When a Sterling Connect:Enterprise HTTP event is complete, it first searches the cehttp/html directory for an HTML file with a specific name. If this file does not exist, Sterling Connect:Enterprise HTTP displays the default HTML file associated with the event.

For example, after a successful logon, Sterling Connect:Enterprise HTTP searches the cehttp/html directory for a file named MSG_LOGON_SUCCESSFUL.htm. If this file does not exist, Sterling Connect:Enterprise HTTP displays the default HTML file associated with a successful logon:

```
Servlet has returned the following message
Logon is successful.
```

You can change this behavior by creating the MSG_LOGON_SUCCESSFUL.htm file in the cehttp/html directory. After a successful logon, Sterling Connect:Enterprise HTTP opens the MSG_LOGON_SUCCESSFUL.htm page rather than the default HTML file. This behavior is called redirection.

You can redirect Sterling Connect:Enterprise HTTP to any HTML code. You can create code that is as simple as displaying simple text, or as complicated as requesting Sterling Connect:Enterprise HTTP to perform additional operations.

To redirect Sterling Connect:Enterprise HTTP, perform the following procedure:

1. Select the event that you want to redirect Sterling Connect:Enterprise HTTP from.
2. Create the HTML file that you want to redirect Sterling Connect:Enterprise HTTP to.
3. Save the HTML file you created in step 2 to the `{WEBSERVER_INSTALL_DIR}/cehttp/html` directory and give it the required HTML file name associated with the event you selected in step 1. Refer to the following table for the required file names:

Event	Required HTML File Name
A directory property file is not readable.	MSG_DIR_FILE_NOT_READABLE.htm
A file is not found.	MSG_FILE_NOT_FOUND.htm
A file is not readable.	MSG_FILE_NOT_READABLE.htm
A format error is encountered.	MSG_FORMAT_ERROR.htm
A remote property file is not found.	MSG_REMOTE_FILE_NOT_FOUND.htm
A remote property file is not readable.	MSG_REMOTE_FILE_NOT_READABLE.htm
A remote property is used out of context.	MSG_REMOTE_PROPERTY_ONLY.htm
A server property file is not found.	MSG_SERVER_FILE_NOT_FOUND.htm
A server property file is not readable.	MSG_SERVER_FILE_NOT_READABLE.htm
An I/O error is encountered.	MSG_IO_ERROR.htm
An invalid server IP address is detected.	MSG_SERVER_IP_INVALID.htm
An invalid server port is detected.	MSG_SERVER_PORT_INVALID.htm
Batch (file) receive failed.	MSG_RECEIVE_FAILED.htm

Event	Required HTML File Name
Batch (file) send failed.	MSG_SEND_FAILED.htm
Cannot connect to server.	MSG_CONNECT_FAILED.htm
Cannot create an instance.	MSG_CREATE_INSTANCE_ERROR.htm
Cannot set timeout.	MSG_SET_TIMEOUT_ERROR.htm
Class cannot be dynamically loaded.	MSG_NO_CLASS.htm
Clear channel control command has failed.	MSG_CCC_ERROR.htm
Default Mailbox server does not exist.	MSG_DEFAULT_SERVER_ERROR.htm
Directory property file is not found.	MSG_DIR_FILE_NOT_FOUND.htm
Download confirmation required but not implemented on Sterling Connect:Enterprise server.	MSG_DOWNLOAD_CONFIRMATION_REQUIRED
Error occurred loading KeyCert file.	MSG_SSL_KEYCERT_FAILED.htm
Error occurred loading trusted root file.	MSG_SSL_ROOT_FAILED.htm
Invalid batch ID detected.	MSG_BATCHID_FAILED.htm
Invalid port range detected.	MSG_INVALID_PORT_RANGE.htm
Invalid request, bad parameters.	MSG_INVALID_REQUEST.htm
Invalid timeout value entered.	MSG_TIMEOUT_VALUE_INVALID.htm
Logoff is successful.	MSG_LOGOFF_SUCCESSFUL.htm
Logon failure	MSG_LOGON_FAILED.htm
No available batches match receive criteria.	MSG_NO_BATCH.htm
No available port found in the specified port ranges.	MSG_PORT_RANGE_ERROR.htm
No cipher suite specified for SSL connection.	MSG_SSL_NO_CIPHER.htm
No file name specified on upload page.	MSG_FILE_NOT_ATTACHED.htm
No user ID is defined.	MSG_NO_USERID.htm
No user ID is specified.	MSG_NO_REMOTE_DEFINED.htm
Send of a file is successful.	MSG_UPLOAD_SUCCESSFUL.htm
Server CONFIRM action failed.	MSG_CONFIRM_FAILED.htm
Server ROLLBACK action failed.	MSG_ROLLBACK_FAILED.htm
Server unknown.	MSG_UNKNOWNHOSTEXCEPTION.htm
SSL connection established.	MSG_SSL_SUCCESSFUL.htm
SSL connection failed.	MSG_SSL_FAILED.htm
The File was received successfully.	MSG_DOWNLOAD_SUCCESSFUL.htm
The HTML page format is incorrect.	MSG_INVALID_HTML_FORMAT.htm
The logon was successful.	MSG_LOGON_SUCCESSFUL.htm

Event	Required HTML File Name
The server has been notified that the file requested was NOT received.	MSG_ROLLBACK_SUCCESSFUL.htm
The server has been notified that the file was successfully received.	MSG_CONFIRM_SUCCESSFUL.htm
Transmission failed.	MSG_TRANSMISSION_FAILED.htm
Transmission failed.	MSG_TRANSMISSION_FAILED_UNKNOWN.htm
Unable to connect to remote FTP server	MSG_INITIAL_CONNECTION_CLOSED
Unknown error.	MSG_ERROR.htm
Unknown FTP server error	MSG_FTP_INTERNAL_ERROR
User is not logged on.	MSG_NOT_LOGGED_ON.htm
You have to enter a new password.	MSG_PWD_ZERO_LENGTH.htm
You have to select a new password that is different from the current password.	MSG_NEWPWD_MATCH_OLD.htm
Your current password is not a valid password. Please try again.	MSG_INVALID_CURRENT_PWD.htm
Your new password does not match the re-entered new password. Please try again.	MSG_NOT_MATCH_PWD.htm
Your password has been successfully changed.	MSG_CHGPWD_SUCCESSFUL.htm
Your password has expired; please change your password now.	MSG_PWD_EXPIRED.htm
Your password has not been changed, contact system administrator for further information. (Note: This will fail if the current password was not valid.)	MSG_CHGPWD_FAILED.htm
Your password has not been changed, contact system administrator for further information. You can still log on with your original password.	MSG_CHGPWD_FAILED_USER.htm

Localizing the User Interface

Sterling Connect:Enterprise HTTP is designed to allow you to localize the application, that is, customize the language for all screens and messages. IBM provides translations into many different languages in the `./webapps/cehttp/html/translations` directory. You can also incorporate your own translations into the product.

Installing a Translation Package

To use Sterling Connect:Enterprise HTTP in a language other than English, you must locate the `.zip` archive file in the `./webapps/cehttp/html/translations` directory for your language and locale, copy the individual files from the `.zip` file to the correct locations, and make a few configuration changes.

Available Translations

These translations are supplied in the `./webapps/cehttp/html/translations` directory:

.Zip archive file	Language	Locale
CEHTTP_da_DK.zip	Danish (da)	Denmark (DK)
CEHTTP_de_DE.zip	German (de)	Germany (DE)
CEHTTP_en_US.zip	English (en)	United States (US)
CEHTTP_es_ES.zip	Spanish (es)	Spain (ES)
CEHTTP_es_MX.zip	Spanish (es)	Mexico (MX)
CEHTTP_fr_FR.zip	French (fr)	France (FR)
CEHTTP_it_IT.zip	Italian (it)	Italy (IT)
CEHTTP_ja_JP.zip	Japanese (ja)	Japan (JP)
CEHTTP_nl_NL.zip	Dutch (nl)	Netherlands (NL)
CEHTTP_no_NO.zip	Norwegian (no)	Norway (NO)
CEHTTP_pt_BR.zip	Portuguese (pt)	Brazil (BR)
CEHTTP_sp_MX.zip	Spanish (sp)	Mexico (MX)
CEHTTP_sv_SE.zip	Swedish (sv)	Sweden (SE)

Copying the Files

You must copy the individual files contained within the `.zip` file to the appropriate locations within the `cehttp` directory structure.

To copy the files, complete the following steps:

1. Make a copy of the existing `{WEBSERVER_INSTALL_DIR}/cehttp/html` directory to prevent overwrite.
2. Copy all `.htm` files from the `.zip` file to the `cehttp/html` directory. Copy all `.jsp` files from `.zip` file to the `cehttp/jsp` directory.
3. Navigate to the `cehttp/WEB-INF/classes` directory.
4. Copy the property file named **message** for your language from the `.zip` file to this directory.

Changing the Configuration

1. Navigate to the following directory, where `WEB_SERVER_ROOT_DIR` is the directory where your Web server is installed:

```
WEB_SERVER_ROOT_DIR/webapps/cehttp/WEB-INF
```

Note: Some web servers read configuration files from a different location than they are originally deployed to. Whenever possible, configure the `web.xml` Initialization Parameters through the console interface for the web server instead of manually editing the file.

2. Edit the `web.xml` file by changing the country code and the language code to the language you are using.

Available language codes are:

Language	Code
Danish	da
Dutch	nl
English	en
French	fr
German	de
Italian	it
Japanese	ja
Norwegian	no
Portuguese	pt
Spanish	es
Swedish	sv

Available country codes are:

Country	Code
Canada	CA
Denmark	DK
France	FR
Germany	DE
Great Britain	GB
Italy	IT
Japanese	JP
Mexico	MX
Netherlands	NL
Norway	NO
Portugal	PT
Spain	ES
Swedish	SE
United States	US

3. Restart your Web server or servlet and verify the changes.
 - ♦ Verify that all buttons, Web pages, and return messages are displayed in the correct language.
 - ♦ Verify the format of dates, time stamps, and other elements in the directory listing.

Creating a New Translation

To create a translation for a new language or locale, download all the files under the Translator Instructions heading on the Sterling Connect:Enterprise HTTP download site. Follow the instructions in the Sterling Connect:Enterprise HTTP localization document listed as Translator Instructions.

Monitoring Sterling Connect:Enterprise HTTP

Sterling Connect:Enterprise HTTP uses two methods of monitoring the processing flow of data within the system: tracing and logging. Both methods occur on the Web server running the Sterling Connect:Enterprise servlet engine and the Sterling Connect:Enterprise HTTP software.

Logging Sterling Connect:Enterprise HTTP Activity

Logging refers to a server function that, when activated, records transmissions and information that is generated while the servlet engine is processing requests. The recorded information includes who is logged in, where they are logged in, specific FTP information, and what error occurred.

The logging process is initialized when the servlet engine is started, and the servlet continues to monitor information until the servlet engine is stopped. Unlike the trace file, the log file does not refresh when the servlet engine is restarted. If you are using JRun, the log file is found at `jrun\jsm-default\services\jse\logs\event.log`.

1. For the UNIX and Microsoft Windows operating systems, navigate to the following directory. Replace `{WEBSERVER_ROOT_DIR}` with the name of the directory where cehttp is deployed.

`{WEBSERVER_INSTALL_DIR}/cehttp/WEB-INF`

2. Open the web.xml file.
3. Edit the file by changing the debug parameter value to one of the following:

Level	Description
0	Initialization messages, all errors
1	Logon / Logoff
3	High-level command - (directory, upload, download, status, for example)
5	FTP chit-chat
6	Directory listings
7	Redirection checking
8-9	For more invasive tracing

Following is an example for the UNIX and Microsoft Windows operating systems:

```
<init-param>
  <param-name>logging</param-name>
  <param-value>1</param-value>
</init-param>
```

4. Save the file.

Because the log file is not refreshed, it can grow very large. If you activate logging, you must maintain this file to keep your system running efficiently. The best way to manage the log file is to open the file in a text editor and move the existing logs to a new file. Save the new file to a location where you plan on storing your log information.

Tracing Sterling Connect:Enterprise HTTP Activity

Tracing is unique to Sterling Connect:Enterprise HTTP and refers to a system function that, when activated, records all method calls and other information. Under normal circumstances, do not activate tracing. If tracing is necessary, contact a IBM Customer Service Representative before activating the feature.

When activated, the tracing process starts when the Sterling Connect:Enterprise servlet starts. Sterling Connect:Enterprise HTTP gathers information until the Sterling Connect:Enterprise HTTP servlet is stopped. All data recorded is stored in the *Installation_Directory*\cehttp folder in a file named **trace**. When you restart the servlet engine, the trace file automatically refreshes and old trace data is lost.

Perform the following procedure to trace Sterling Connect:Enterprise HTTP activity:

1. For the UNIX and Microsoft Windows operating systems, navigate to the following directory. Replace *{WEBSERVER_ROOT_DIR}* with the name of the directory where cehttp is deployed.

```
{WEBSERVER_INSTALL_DIR}/cehttp/WEB-INF
```

2. For the UNIX and Microsoft Windows operating systems, open the web.xml file.
3. Edit the file by changing the debug parameter value to one of the following:

Value	Description
0	Tracing disabled
1-2	Unused
3	Tracing enabled

Following is an example:

```
<init-param>
  <param-name>debug</param-name>
  <param-value>3</param-value>
</init-param>
```

4. Save the file.

5. Perform the operations that you want to trace.
6. Rename the **trace** file located in directory where cehttp is deployed and save it to a location where you want to store historical trace information.

If you do not frequently restart the Web application, your trace information can grow dramatically in size. Manage the size of this file by opening the file in a text editor and moving the existing trace information to a new file. Save the new file to a location where you plan on storing your trace information.

Appendix A

Error Messages

This appendix explains error messages related to Sterling Connect:Enterprise HTTP.

Logon Messages

The system returns the following error messages based on different logon conditions:

Message	Condition	Action
Cannot connect to the server.	The <i>ftpd</i> is not monitoring the port specified, or the server is down.	Contact your system administrator to verify that the Sterling Connect:Enterprise server is up and running on the specified port.
Cannot connect to the Sterling Connect:Enterprise server.	After exhausting the numbers in the port ranges specified in the property file, no valid socket could be created.	Contact your system administrator to verify the available port ranges on the server and change the value of the <code>port_range</code> attribute to include the available port ranges.
Cannot find remote property file.	The Remote property file as entered or specified by the system administrator cannot be found.	Verify that you are entering the correct user ID when logging on.
Cannot find server file.	A value was typed into the Sterling Connect:Enterprise server field that does not match the file names in the server property directory. This error can also occur if file names are not included in the Sterling Connect:Enterprise server field, and the default server file is not in the Server property file directory.	Contact your system administrator to verify that the Server property file is in place.
Cannot find directory property file.	The Directory property file cannot be found as entered or specified by the system administrator.	Contact your system administrator to check for the existence of the file and make sure it is readable.
Cannot open directory property file.	The Directory property file is specified, but cannot be opened. Either the file does not exist, or the file is not readable.	Contact your system administrator to check for the existence of the file and make sure it is readable.

Message	Condition	Action
Cannot open remote property file.	The Remote property file cannot be opened.	Contact your system administrator to check for the existence of the file and make sure it is readable.
Cannot open server property file.	The Server property file is specified, but cannot be opened. Either the file does not exist or file is not readable.	Contact your system administrator to check for the existence of the file and make sure it is readable.
Cannot set time_out.	An error occurred while trying to set the socket time_out.	Contact your system administrator to reinitialize the servlet engine by restarting it. If reinitialization fails, restart the Web server.
Clear control channel command failed.	FTP Clear Control Channel (CCC) command failed to turn off encryption.	Contact your system administrator
Sterling Connect:Enterprise server hostname/IP address is invalid.	The hostname/IP address you are trying to connect to is invalid.	Contact your system administrator to verify that the keyword address in the Server property file has the proper value.
Sterling Connect:Enterprise server port number is invalid.	The Server property file does not have a port line or the port is not valid. A test is performed on the port if the value is an integer between 1 and 65535. In all other cases, this error is returned.	Contact your system administrator to type the correct port number in the Server property file.
Default Sterling Connect:Enterprise server does not exist.	Nothing was typed in the Sterling Connect:Enterprise server field and the Mailbox_server value is not valid in the System property file or in the Remote property file.	Contact your system administrator to set up a default Sterling Connect:Enterprise server.
Invalid request.	A customized Web page does not contain hidden field operations with proper values.	Contact your system administrator to verify the parameters entered on the HTML form. Make sure that the value for operation is LOGON.
No available port found in the specified ranges.	Port ranges specified in the port_range attribute of the Server property file do not include a port on the server.	Contact your system administrator to change the port_range attribute to include port number available on the server.
No remote value defined.	The remote value is either not defined or cannot be recognized.	Type a valid user ID.
No user ID is specified.	You did not specify a user ID.	Specify a user ID and try again, or contact the system administrator to set up a default remote value in the System property file, or allow the you type one on the log on screen.
Only a user with a remote property file defined can access Sterling Connect:Enterprise server.	Either the user ID field entry does not match the file in the remote directory, and the defined_remote_only value is Y, or the user ID field is empty, the remote field does not exist, and the defined_remote_only value is Y.	Contact your system administrator to set up the account.
Server Unknown.	The hostname/IP address you are trying to connect to is invalid.	Contact your system administrator to verify that the keyword address in the Server property file has the proper value.

Message	Condition	Action
Time-out value entered is not valid.	The value for time_out is not valid.	Contact your system administrator to verify that the value for the keyword <code>session_timeout</code> in the System property file is a positive integer.
You are not logged on to a server. Please log on first.	You sent a request before logging on or after the you were logged off because of a system time-out.	Log on, then attempt your request again.
Your password has expired. Please change your password now.	Your current password has expired.	Change your password.

Change Password Messages

The system returns the following error messages based on change password conditions:

Message	Condition	Action
You are not logged on to a server. Please log on first.	You clicked Change Password before you successfully logged on.	Log on, then attempt to change your password.
You have to enter a new password.	You attempted to change your password, but did not enter a new password.	Attempt to change your password and provide a new password.
You have to select a password that is different from the current password.	You attempted to change your password using your current password.	Attempt to change your password again and provide a new password that is different from your current password.
Your password has expired; please change your password now.	Your current password has expired.	Change your password.
Your current password is not a valid password. Please try again.	When you attempted to log on, you typed an incorrect password.	Attempt to log on again, using the correct password. Contact the system administrator if you do not know your password.
Your new password does not match the reentered password.	The values you typed for New Password and Verify Password are not the same.	Attempt to change your password again, make sure that you type the same values for New Password and Verify Password.
Your password has not been changed, contact system administrator for further information.	The system prompted you to change your password, and your attempt to change your password failed.	Contact your system administrator.
Your password has not been changed, contact system administrator for further information. You can still log on with your current password.	Your attempt to change your password failed.	Log on with your current password and contact your system administrator.

Directory Messages

The system returns the following error messages based on different directory request conditions:

Message	Condition	Action
Cannot find the directory property file.	The system cannot find the Directory property file as it is entered or specified.	Contact your system administrator to check for the existence of the file and make sure it is readable.
Class cannot be dynamically loaded.		Contact your system administrator to verify the correct MailboxServlet.jar file.
Cannot create an instance.	The class may be missing.	Contact your system administrator. When the class is dynamically loaded, a new instance is created. If an error occurs while an instance is being created, try to restart the servlet engine. If restarting the servlet engine fails, restart the Web server.
Invalid request.	A customized Web page does not contain hidden field operations with proper values.	Contact your system administrator to verify the parameters entered on the HTML form. Make sure that the value for operation is DIRECTORY.
No batch available matches your receiving criteria.	This error occurs when there is no batch in the mailbox ID specified, or no batch satisfies the criteria provided.	Verify that the batch requested is available for viewing.
There is a format error.	The return format from dir \$\$ command is not correct. This message is displayed on UNIX only.	Contact your system administrator to verify that the format settings on the Sterling Connect:Enterprise server are correct.
There is an I/O error.	A write error occurs during the ftp session or http session.	Retry the request. If it still fails, contact your system administrator to verify that the directory format settings on the Sterling Connect:Enterprise server are correct.

Send Messages

The system returns the following error messages based on different send conditions:

Message	Condition	Action
Attempt to Close with Data Remaining.	You attempted to send a binary file but indicated that it was an ASCII file.	Resend the file and correctly specify the file type.

Message	Condition	Action
Class cannot be dynamically loaded.		Contact your system administrator to verify that the correct MailboxServlet.jar file is in the JRun/Servlets directory.
File name has not been specified.	You did not type a file name in the Send File Name field and press Send.	Resend the file and verify that you have typed a file name in the file name field.
Invalid batch id detected.	The batch ID specified in the send was too long, or did not match a batch ID on the server.	Correct the batch ID.
Invalid request.	A customized Web page does not contain hidden field operations with proper values.	Contact your system administrator to verify the parameters entered on the HTML form. Make sure that the value for operation is UPLOAD.
Send failed.	Your send request failed due to file permission issues.	Submit the request again. If it still fails, contact your system administrator to check the permissions to verify that you have permission to send files to the mailbox with the ID you specified.
Send failed.	After exhausting the numbers in the port ranges specified in the property file, no valid socket could be created.	Contact your system administrator to verify the available port ranges on the server and change the value of the port_range attribute to include the available port ranges.
There is an I/O error.	A write error has occurred in transmission during the ftp session or http session.	Submit the request again. If it still fails, contact your system administrator to restart the servlet engine, and if needed, restart the Web server.
Parameter not recognized. The following text was not accepted: TRIGGER	You attempted to specify trigger_flag=Y in the property files while sending to a Sterling Connect:Enterprise for z/OS server, which does not support the trigger flag feature.	Specify trigger_flag=N in the system, server, and remote property files and attempt to send the file again.

Receive Messages

The system returns the following error messages based on different receive conditions:

Message	Condition	Action
Class cannot be dynamically loaded.		Contact your system administrator to verify the correct MailboxServlet.jar file.
Invalid request.	A customized Web page does not contain hidden field operations with proper values.	Contact your system administrator to verify the parameters entered on the HTML form. Make sure that the value for operation is DOWNLOAD.

Message	Condition	Action
Receive failed.	After exhausting the numbers in the port ranges specified in the property file, no valid socket could be created.	Contact your system administrator to verify the available port ranges on the server and change the value of the port_range attribute to include the available port ranges.
No available batch matches your receiving criteria.	No batch matches your receive criteria.	Contact your system administrator to verify that the batch requested is available for download.
There is an I/O error.	A read error occurred in transmission during the ftp session or http session.	Submit the request again. If it still fails, contact your system administrator to restart the servlet engine and if needed, restart the Web server.

Other Messages

Symptom	Cause	Resolution
After installing a new version, the old version is still displayed.	You browser is reading the temporary files created from the old version.	When installing a new version, delete all of the temporary files created by your browser.
When you attempt to start the product, you get the message: Unable to find page.	The path defined in web.xml is not correct.	Review Chapter 3, <i>Configuring the Servlet Engine</i> in the <i>IBM Sterling Connect:Enterprise HTTP Installation and Administration Guide</i> for setting up the web.xml file.
The Directory window is not displayed.	RSD file parameter DIRFORM= is not set correctly in the Mailbox Server.	Specify the RSD file parameter DIRFORM=CLIENT in the Mailbox Server.
	UNIX write permissions are not valid.	Set write permissions to the cehttp directory.
Unable to connect to the Mailbox Server.	SSL certificate has expired. (There are no messages when this happens.)	Use Sterling Certificate Wizard to verify the expiration date.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual

Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT,

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA__95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the

examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2011. Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2011.

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce, Inc., an IBM Company.

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

Glossary

A

Applet A program designed to execute from within another application. Unlike an application, you cannot execute applets directly from the operating system.

ASCII American Standard Code for Information Interchange. A standard format used to communicate data between different types of computers. ASCII is the traditional System V coded character set and defines 128 characters, including both control and graphic characters, each of which is represented by 7-bit binary values from 0–127 decimal. An ASCII file created on a UNIX computer is readable on other kinds of computers.

Attribute Characteristics that identify the operation performed and the options for that operation. The attribute values are provided using form fields and hidden parameters within the HTML pages.

B

Batch Attribute Specifies how files are handled after they reach the destination Sterling Connect:Enterprise server.

Batch ID You can complete a parameter with either a batch number or user batch ID entry. See also *batch number* and *user batch ID*.

Batch Number A sequential number between 1 and 9,999,999 assigned internally by Sterling Connect:Enterprise to each batch. You can specify this number using the BATCHID= parameter. Obtain the number by either the \$\$DIRECTORY or the **cmulist** commands. See also *BATCHID* and *user batch ID*.

Binary Data Data that is not in a readable format. For example, executable files are binary data.

C

Class A Java file that is loaded dynamically to expand the functionality of a server. In object-oriented

programming, a category of objects defining all the common properties of the different batches that belong to it.

D

Data Format Designates the file type of the file being sent.

Debugging The process of locating and correcting errors in computer programs.

Directory Request Provides a list of batches from the Sterling Connect:Enterprise data repository by using the HTTP protocol support inherent to most Web browsers.

F

File name The name given to a file. Files in the same directory cannot have the same name, but files in different directories can have the same name.

FTP File Transfer Protocol. The command used to connect to any other computer on your network running FTP. When connected, you can use FTP to transfer files to your computer. Is also used to access files anywhere on the Internet provided you have access to the Internet.

H

HP-UX The Hewlett-Packard implementation of the UNIX operating system.

HTML Hypertext Markup Language. The authoring language used to create documents on the World Wide Web.

HTTP Hypertext Transfer Protocol. The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers take in response to various commands. HTTP is called a stateless protocol because each command is executed independently,

without any knowledge of the commands that came before it.

I

IIS Short for Internet Information Server, the Microsoft Web server that runs on Microsoft Windows.

Initialization Assigns a starting value to a property file key. Used to begin a function within the Sterling Connect:Enterprise HTTP system.

Internet The name for a group of interlinked computer networks that distribute news, electronic mail, and information throughout the world. Currently, the largest computer network system in the world.

Internet address The name given to a computer system that enables it to receive and send Internet news and mail.

Intranet A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by organization members, employees, or others with authorization.

J

Java A general-purpose programming language with a number of features that make the language well suited for use on the World Wide Web. Java is an object-oriented language similar to C++, but simplified to eliminate language features that cause common programming errors.

L

Log A collection of messages placed in an auxiliary storage device for accounting or data collection purposes.

Logging Takes place at the Web server and refers to a server log file that logs information such as who logs in, from where they log in, what time, and what operations are being conducted.

Logon The process of establishing a session between a remote site and a local site program such as Sterling Connect:Enterprise. You can logon automatically after a connection is established, or you can type a logon as

a text command or a control function. In Sterling Connect:Enterprise either the remote site or the local site can start the logon process.

M

Mailbox The file area used to store electronic mail messages.

Mailbox ID A 1–8 character name that identifies Sterling Connect:Enterprise batches. Usually, a single mailbox ID is assigned to each remote site for its exclusive use. The mailbox ID is always specified in the ID= keyword.

P

Parameter A special type of variable used within shell programs to access values related to arguments on the command line or the environment in which the program is executed. Also, an option or variable on the command line that modifies the default action of the command.

Password A value known only to the user that is called for in the login authentication process. The computer uses the password to verify that the user is actually valid and permitted to use the system.

Process Generally, a program that is at some stage of execution. In UNIX, it refers to the execution of a computer environment, including contents of memory, register values, name of the current directory, status of files, information recorded at login time, and various other items.

Property Files Java property files are ASCII files and can be edited with any plain-text editor. They contain sets of key/value pairs. The keys are words, which represent individual properties, and the values are their definitions. Each property is a single logical line within a property file.

R

Record A row in a structured data file. For example, if a user creates a file containing the names, phone numbers, and salary of every employee, with employee information contained in a single row, that row is called a record.

Remote Any terminal, computer, or software that can connect with Sterling Connect:Enterprise through FTP, switched or leased line connections. See also *FTP*.

Receive To download data (usually an entire file) from the Sterling Connect:Enterprise data repository to the servlet.

S

Send The process of copying a file from your own computer to another computer.

Server A computer that serves all the other terminals or computers within a network. The server usually contains additional memory, storage capacity, and printer capabilities enabling it to handle the users to which it is linked.

Servlet A Java applet that runs within a Web server environment, expanding the functionality of a server. A program designed to be executed from within another application. Sterling Connect:Enterprise HTTP is considered a servlet.

Session A logical connection between Sterling Connect:Enterprise at the local site and another computer at the remote site. When a logon command is completed between Sterling Connect:Enterprise and a remote site, the two are said to be in session.

Shell A program that interprets commands from the user into instructions the computer can understand. Popular UNIX shells include the Bourne, Korn, and C shells.

Solaris The Sun Microsystem implementation of the UNIX operating system.

SSL Secure Sockets Layer is a communications system that ensures privacy when communicating with other SSL-enabled products. SSL is a protocol that runs above TCP/IP and below HTTP.

Sterling Connect:Enterprise for UNIX A IBM online telecommunications program that runs in a host computer and manages data collection and data transmission between the host and remote terminals and computers. The system includes command line utilities to manage the batch data storage system. For UNIX, Sterling Connect:Enterprise supports the standard protocols including Bisync, Async and FTP.

String A designation for a particular group or pattern of characters, such as a word or phrase.

Syntax The grammar of a command. How the command line, its variables, and parameters are arranged so that the program or system understands what the user means.

System A combination of components working together. For example, a computer system includes both hardware and software.

System administrator The person officially assigned to oversee housekeeping chores on a computer system, including adding new users, assigning addresses and logon names, scheduling system backups, and maintaining system integrity.

T

TCP/IP Transmission Control Protocol/ Internet Protocol. The suite of communications protocols that connects hosts on the Internet. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

Tracing In Sterling Connect:Enterprise, the ability to create a snapshot of a dump of internal Sterling Connect:Enterprise control information for communications activity, user exit calls, or mailbox access.

U

UNIX A general-purpose, multiuser, interactive, time-sharing operating system developed by AT&T Bell Laboratories. The UNIX system enables several users to share limited computer resources and efficiently organizes the user interface to a computer system.

User Batch ID The 1–64 character free-form batch identifier that the user gives to describe the contents of a batch of data in the Enterprise. Entry is made in the *BATCHID=* parameter. See also *BATCHID* and *batch number*.

User ID In Sterling Connect:Enterprise for UNIX, the name of the RSD file for the local site user.

V

- vi** A text editor packaged with most UNIX systems.

Index

A

address 35
Authentication 24

C

cepassprotect 26
Change Password Messages 59
cipher_strength 30, 36, 40
Client-Server Session 24
Configuring
 Security 23
 Sun ONE 20
 Tomcat
 new installation 19
 upgrade installation 20
 WebSphere for UNIX 22
Conventions 8
Cryptography 24
Customizing the user interface 45

D

data_format 30, 40
defined_remotes_only 30
description 36, 40, 43
directory 36, 40
Directory Messages 60
Directory property files 42
directory_in_memory 31
Documentation 9
download_confirm_mode 36
download_status 36

E

enable_download_status_file_size 36

F

FTP 13
ftp_passive_mode 36
Functions 12
 log on 12
 receive 12
 send 12

H

HTML pages
 customizing 45

I

Installing Sterling Connect:Enterprise HTTP on Microsoft Windows 15
Installing Sterling Connect:Enterprise HTTP on the UNIX OS 14

K

Key Certificate File 25
keycert_file 31, 36, 40

L

Localizing Sterling Connect:Enterprise HTTP 49
Log on Messages 57
logging 53

M

mailbox_id 31, 40

mailbox_server 31, 41

Messages 57

Change Password 59

Directory 60

Log on 57

Receive 61

Send 60

Monitoring 53

multiple_download 37

N

notational conventions 8

P

pfcheck 28

port 37

port_range 37

port_retries 37

port_retry_wait_time 37

Property files 27

directory 42

description 43

show_batch_id 43

show_batch_num 43

show_cezos_record_count 43

show_cezos_vbqidt 43

show_creation_date 43

show_creation_time 43

show_data_format 43

show_deleted_batches 44

show_flags 44

show_mailbox_id 44

show_originator_id 44

show_size 44

show_unrequestable_batches 44

overview 27

port_range 37

port_retries 37

port_retry_wait_time 37

remote 39

data_format 40

description 40

directory 40

keycert_file 40

mailbox_id 40

mailbox_server 41

password 41

root_cert_file 41

ssl_passphrase 41

trigger_flag 41

user_id 41

server

address 35

cipher_strength 36, 40

description 36

directory 36

download_confirm_mode 36

download_status 36

enable_download_status_file_size 36

ftp_passive_mode 36

keycert_file 36

multiple_download 37

overview 33

port 37

root_cert_file 37

security_policy 37, 41

ssl_client_ccc_policy 38

ssl_passphrase 38

trigger_flag 38

zip_entry_format 38

system 29

cipher_strength 30

data_format 30

defined_remotes_only 30

directory 30

directory_in_memory 31

keycert_file 31

mailbox_id 31

mailbox_server 31

remote 31

root_cert_file 31

security_policy 31

servlet_info 31

session_timeout 32

ssl_passphrase 32

R

Receive Messages 61

Redirecting Sterling Connect:Enterprise HTTP 47

remote 31

Remote property files 39

root_cert_file 31, 37, 41

S

Security 23
 security_policy 31, 37
 Send Messages 60
 servlet_info 31
 session_timeout 32
 show_batch_id 43
 show_batch_num 43
 show_cezos_record_count 43
 show_cezos_vbqid 43
 show_creation_date 43
 show_creation_time 43
 show_deleted_batches 44
 show_flags 44
 show_mailbox_id 44
 show_originator_id 44
 show_size 44
 show_unrequestable_batches 44
 SNA 13
 SSL Passphrase 26
 ssl_client_ccc_policy 38
 ssl_passphrase 32, 38
 Sterling Connect:Enterprise Gateway 11
 Sun ONE 20
 System property file 29

T

TCP/IP 13
 tracing 54
 trigger_flag 38, 41

U

Uninstalling Sterling Connect:Enterprise
 HTTP 16, 17
 Upgrading Sterling Connect
 Enterprise HTTP on the UNIX OS 14
 Upgrading Sterling Connect:Enterprise HTTP on a
 Microsoft Windows NT/2000/XP OS 16

User interface 45
 user_id 41

W

WebSphere for UNIX 22

Z

zip_entry_format 38

