

# **IBM Sterling Connect:Enterprise for UNIX**

## **Installation and Administration Guide**

**Version 2.5**



This edition applies to the 2.5 Version of IBM® Sterling Connect:Enterprise® for UNIX 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 309.

Licensed Materials - Property of IBM

IBM® Sterling Connect:Enterprise® for UNIX

© Copyright IBM Corp. 2004. 2011. All Rights Reserved.

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

---

# Contents

<b>Chapter 1 About Sterling Connect:Enterprise for UNIX</b>	<b>11</b>
Transmitting and Collecting Data . . . . .	11
Sterling Connect:Enterprise for UNIX Terminology . . . . .	12
Sterling Connect:Enterprise Features . . . . .	14
Sterling Connect:Enterprise for UNIX Site Administration User Interface . . . . .	15
Sterling Connect:Enterprise Software . . . . .	16
Sterling Connect:Enterprise for UNIX Documentation . . . . .	17
About This Guide . . . . .	17
Task Overview . . . . .	18
<b>Chapter 2 Installing Sterling Connect:Enterprise for UNIX</b>	<b>21</b>
Before You Begin . . . . .	21
Creating the User ID . . . . .	23
Installation Script Conventions . . . . .	23
Starting the Installation Script . . . . .	24
Installing All Sterling Connect:Enterprise for UNIX Components . . . . .	25
Installing Sterling Connect:Enterprise for UNIX Base . . . . .	26
Customizing Sterling Connect:Enterprise for UNIX . . . . .	30
Setting Up Secure FTP . . . . .	30
Setting Up SSH . . . . .	32
Configuring High Availability . . . . .	34
Setting Up AS2 . . . . .	35
Setting Up the HTTP Server . . . . .	36
Completing the Installation . . . . .	37
Installing Sterling Connect:Enterprise Remote Daemons . . . . .	39
Installing Sterling Connect:Direct for UNIX . . . . .	42
Configuring Sterling Connect:Enterprise File Agent, MQ Agent, and cereport . . . . .	42
Configuring File Agent . . . . .	43
Configuring MQ Agent . . . . .	45
Configuring cereport . . . . .	45
<b>Chapter 3 Upgrading Sterling Connect:Enterprise for UNIX</b>	<b>47</b>
Upgrade Considerations for Version 2.4.04 . . . . .	47
New Encryption Ciphers for Password and Stored Batch Encryption . . . . .	47
Global Key Changes . . . . .	48

Password Encryption Changes . . . . .	48
Stored Batch Encryption Changes . . . . .	49
Upgrade and Fallback Planning . . . . .	49
Upgrade Considerations for Version 2.4.03 and Earlier . . . . .	50
Encryption of Inbound AS2 Batches . . . . .	50
Correlation of AS2 Batches . . . . .	50
Running the Installation Script . . . . .	50
Customizing Sterling Connect:Enterprise for UNIX . . . . .	55
Completing the Installation . . . . .	56

**Chapter 4 Post-Installation Tasks 57**

---

Exporting the Environment Variables . . . . .	57
Testing the Installation . . . . .	59
Remove userid.log Files . . . . .	65
Setting Up the Sterling Connect:Enterprise for UNIX Site Administration User Interface . . . . .	65
Configuring Role-Based Access . . . . .	67

**Chapter 5 Starting and Stopping Sterling Connect:Enterprise 69**

---

Startup Script . . . . .	69
Starting Sterling Connect:Enterprise with ceustartup . . . . .	69
Starting Sterling Connect:Enterprise in Debug Mode . . . . .	71
Modifying Startup Scripts . . . . .	72
Configuring FTP to Use SOCKS Protocol . . . . .	73
cmuctld—Control Daemon . . . . .	73
cmuctld Parameters . . . . .	74
cmuauthd—Authentication Server Daemon . . . . .	75
cmumboxd—Mailbox Daemon . . . . .	76
cmumboxd Parameters . . . . .	76
cmulogd—Log Daemon . . . . .	78
cmulogd Parameters . . . . .	78
cmuacd—Auto Connect Daemon . . . . .	79
cmuacd Parameters . . . . .	80
cmuexitd—Exit Daemon . . . . .	81
cmuexitd Parameters . . . . .	81
cmusvid—Service Interface Daemon . . . . .	82
cmuadmind—Administration Daemon . . . . .	84
cmuasyd—Async Daemon . . . . .	85
cmuasyd Parameters . . . . .	86
cmuftpd—FTP Daemon . . . . .	87
cmuftpd Parameters . . . . .	88
Modifying the Signon Banner . . . . .	91
cmusshftpd—SSH Daemon . . . . .	92
cmusshftpd Parameters . . . . .	92
cmubscda—Bisync Daemon for ARTIC Card . . . . .	94
cmubscda Parameters . . . . .	95
cmubscdc—Bisync Daemon for Cleo SYNCcable+ Hardware . . . . .	96

cmuhttpd—HTTP Daemon for AS2 . . . . .	98
Timeout for the HTTP Daemon . . . . .	99
cmuediintd—EDIINT Daemon for AS2 . . . . .	99
Shutting Down Sterling Connect:Enterprise . . . . .	101
ceushutdown Format . . . . .	101
ceushutdown Output . . . . .	101
ceushutdown Parameters . . . . .	101
Shutting Down Sterling Connect:Enterprise Base . . . . .	102
cmushutdown Format . . . . .	102
cmushutdown Parameters . . . . .	103
<b>Chapter 6 Role-Based Access</b>	<b>105</b>
<hr/>	
About Role-Based Access . . . . .	105
Designing a Single-Level Role-Based Access System . . . . .	105
Designing a Multilevel Role-Based Access System . . . . .	107
Resource Permissions . . . . .	108
Role Permissions . . . . .	110
<b>Chapter 7 Password Administration</b>	<b>113</b>
<hr/>	
Configuration File . . . . .	114
Password Policy Files . . . . .	115
RSD Policy Files . . . . .	116
Creating and Maintaining Password Policy Files . . . . .	116
Creating a Password Policy . . . . .	119
Forcing Password Change at Logon . . . . .	120
Displaying Policy File Contents . . . . .	121
Applying All Password Flags . . . . .	121
Applying a Password Policy to a Bulk File . . . . .	121
Generating RSD Policy Reports . . . . .	122
Changing User Password . . . . .	124
Authentication Log File . . . . .	125
<b>Chapter 8 Administrator Commands</b>	<b>127</b>
<hr/>	
Generating the Global Key (ceukey) . . . . .	127
Creating a Global Key . . . . .	128
Encrypting RSD Passwords . . . . .	129
Changing the Passphrase of the Global Key . . . . .	130
Replacing Your Global Key . . . . .	130
Creating SSH SFTP Keys (cmusshkey) . . . . .	131
Create a Host Key Pair . . . . .	132
Create an RSD Key . . . . .	132
Change the Passphrase on a Private Key . . . . .	132
Encrypting Existing Passwords (ceupassencrypt) . . . . .	133

Locating Configuration Problems (cmucheckcfg) . . . . .	134
Correcting Control File Records (cmufixup) . . . . .	134
Initializing a Mailbox (cmuinit) . . . . .	136
Reconstructing Repository Control Files (cmurebuild) . . . . .	137
Reclaim Space and Improve Performance . . . . .	137
Rebuilding the Repository Database . . . . .	138
Tracing Sterling Connect:Enterprise Activity . . . . .	139
Turning Tracing On . . . . .	139
Daemon Considerations . . . . .	143
Locating Your Trace Files . . . . .	144
Clearing and Restarting Your Trace Files . . . . .	144
Examples . . . . .	145
ceukey Example . . . . .	145
ceupassencrypt Example . . . . .	145
cmucheckcfg Example . . . . .	145
cmufixup Examples . . . . .	146
cmurebuild Example . . . . .	146
cmuinit Example . . . . .	146
cmrebuild Example . . . . .	147

---

**Chapter 9 Generating Reports 149**

cmureport Utility . . . . .	149
Auto Connect Detail Report . . . . .	156
Auto Connect Summary Report . . . . .	158
Remote Connect Detail Report . . . . .	159
Remote Connect Summary Report . . . . .	160
Queued Auto Connect Report . . . . .	161
Offline Utilities Log Report . . . . .	162
AS2 Report . . . . .	163
Displaying Pipe-Delimited AS2 Reports . . . . .	163

---

**Chapter 10 Configuring Secure FTP 165**

Sterling Connect:Enterprise Secure FTP Features . . . . .	165
Cryptography . . . . .	165
Configuring Secure FTP . . . . .	167
Establishing the Security Policy . . . . .	167
Obtaining and Installing Your Certificate . . . . .	169

---

**Chapter 11 Configuring SSHFTP Protocol 173**

Configuring Sterling Connect:Enterprise SSH Server . . . . .	173
Configuring a Remote SSHFTP Client Connection . . . . .	174

---

## Chapter 12 Configuring AS2 177

About AS2 .....	177
Sending from Sterling Connect:Enterprise to a Trading Partner .....	178
Receiving AS2 Messages from a Trading Partner .....	179
AS2 Messages Requesting Async MDNs .....	179
AS2 Messages Requesting Sync MDNs .....	180
Configuring Sterling Connect:Enterprise for UNIX for AS2 .....	181
Configuring the AS2 Port .....	182
Configuring the HTTP Proxy .....	183
Creating the AS2 Contract .....	183
Identity Information Worksheet .....	183
SSL Information Worksheet .....	184
Digital Signature Information Worksheet .....	185
Exchange Encrypted Messages Information Worksheet .....	185
Message Options Worksheet .....	186
Retry of Outbound AS2 Connections .....	187
For AS2 Messages Requiring an MDN .....	187
For Outbound Asynchronous MDNs .....	187
For AS2 Messages Not Requiring an MDN .....	188

---

## Chapter 13 Configuring WebDAV Protocol 189

---

## Chapter 14 Configuring the External Authentication Service 191

Determine What Procedures to Follow .....	192
Configuring the SSL Credentials for Connection .....	192
Specify the Path to Keytool .....	192
Change the Default Passphrases for the External Authentication Service .....	193
Create a Key/Certificate for the External Authentication Service .....	195
Export the External Authentication Service Certificate to Sterling Connect:Enterprise .....	196
Create a Key/Certificate for Sterling Connect:Enterprise .....	197
Import the Sterling Connect:Enterprise Certificate to the External Authentication Service Truststore .....	197
Start Sterling Connect:Enterprise and the External Authentication Service .....	198
Create and Identify a Security Definition for the External Authentication Service .....	199
Enable the Secure Access Acceptor .....	200
Restart and Verify the Secure Connection .....	201
Define the Server Access Definition .....	202
Disable the Nonsecure Port (Optional) .....	202
Changing Your Keystore Password After Your Key/Certificate Is Added (Optional) .....	202

## Chapter 15 Running Protocol Daemons on Remote Servers 205

---

Firewall Considerations . . . . .	205
Installing the Remote Daemons . . . . .	206
Configuring SSL for AS2 . . . . .	206
Configuring SSL for WebDAV . . . . .	210

## Chapter 16 Configuring High Availability 215

---

Installing Sterling Connect:Enterprise High-Availability Scripts . . . . .	215
Customizing Sterling Connect:Enterprise for the High-Availability Feature . . . . .	215
Configuring Protocol Daemons for the High-Availability Feature . . . . .	216
Sterling Connect:Enterprise Core High-Availability Scripts . . . . .	217
Syntax and Parameters for the proc_mon.cfg Script . . . . .	218
Arguments for the ce_ha_probe Script . . . . .	219
Using Core Scripts without Implementing High Availability . . . . .	220
Sun Solaris High-Availability Implementation . . . . .	220
Resource Type Registration File . . . . .	221
Configuring the ce_svc_start and ce_svc_stop Scripts . . . . .	221
Configuring the ce_svc_probe Script . . . . .	222
Registering Sterling Connect:Enterprise with the Sun Package Manager . . . . .	222
Commands Used with the Sun Solaris High-Availability Implementation . . . . .	222
Hewlett-Packard High-Availability Implementation . . . . .	223
High-Availability Scripts . . . . .	223
Configuration Files . . . . .	224
Configuring Sterling Connect:Enterprise for the HP High-Availability Environment . . . . .	227
Setting Up Sterling Connect:Enterprise for a Two-Node MC/ServiceGuard Cluster . . . . .	228
Setting Up Sterling Connect:Enterprise on the hp1 Node . . . . .	228
Setting Up the hp2 Node . . . . .	229
Configuring the MC/ServiceGuard Cluster . . . . .	229
Configuring the ServiceGuard Package on a Single Node . . . . .	230
Adding the Second Node to the ServiceGuard Package . . . . .	231
Sample Output of the cmviewcl Command . . . . .	231
Commands Used with the Hewlett-Packard High-Availability Implementation . . . . .	232
AIX High-Availability Implementation . . . . .	233
Configuring the Sterling Connect:Enterprise AIX High-Availability Scripts . . . . .	233
Registering Sterling Connect:Enterprise with the AIX Package Manager . . . . .	234
Adding a Resource Group . . . . .	235
Adding an Application Server . . . . .	235
Changing or Showing Resources or Attributes for a Resource Group . . . . .	236
Synchronizing Cluster Resources . . . . .	236



<b>Chapter 17 Encrypting Internal Product Communications</b>	<b>237</b>
Enabling Message Encryption . . . . .	237
Configuring for Sterling Connect:Enterprise Components Running on Different Computers . . . . .	238
Configuring for Components Connecting to Multiple Sterling Connect:Enterprise Instances . . . . .	238
<b>Appendix A Error Messages</b>	<b>239</b>
Sterling Connect:Enterprise Error Codes . . . . .	240
API Error Codes . . . . .	247
Auto Connect Status Codes . . . . .	249
Remote Connect Status Codes . . . . .	251
Utilities Exit Codes . . . . .	253
Authorization Log Message IDs . . . . .	253
Policy File Entries . . . . .	255
Rsdpolicy File Entries . . . . .	256
Account Lock-Related Entries . . . . .	256
Policy Level Entries . . . . .	257
Password Change Entries . . . . .	257
Additional Return Codes for AUTH0113 . . . . .	262
<b>Appendix B Translation Table Format</b>	<b>265</b>
<b>Glossary</b>	<b>267</b>
<b>Index</b>	<b>303</b>
<b>Notices</b>	<b>309</b>
Trademarks . . . . .	311



---

# About Sterling Connect:Enterprise for UNIX

IBM® Sterling Connect:Enterprise® is an online data communications system developed by IBM for use with large networks within a UNIX environment. Sterling Connect:Enterprise enables the exchange of information between and within companies, including unattended, automatic data collection and distribution.

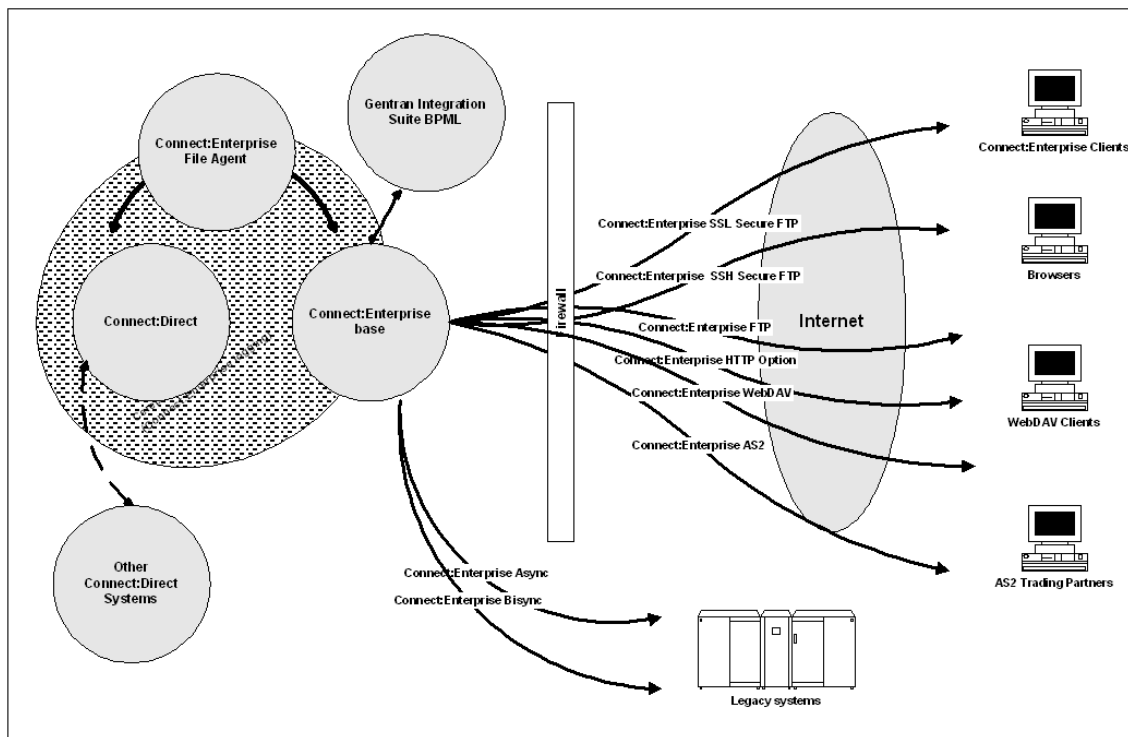
Sterling Connect:Enterprise supports Bisync, Async, FTP, Secure FTP, HTTP, WebDAV, SSH-2, AS2 protocols, IBM® Sterling B2B Integrator business processes, and IBM® Sterling Connect:Direct® Processes. It provides open connections throughout the network to any host, client/server, or remote workstation.

Refer to the *IBM Sterling Connect:Enterprise for UNIX Version 2.5.00 Release Notes* for release-specific information.

---

## Transmitting and Collecting Data

Sterling Connect:Enterprise for UNIX collects and transmits data between the host computer and remote terminals, applications, or computers through the *data repository*, which is designed on the store and forward model. Like a voice mail system, the data repository consists of individual *mailboxes*, or directories, where data files are stored for future processing by the host or remote site. The Sterling Connect:Enterprise administrator assigns mailboxes and controls access to the mailboxes through Sterling Connect:Enterprise for UNIX user IDs and passwords. After a communications session is established between Sterling Connect:Enterprise for UNIX and a remote site, either the host or the remote users can store, retrieve, or monitor data files in the mailboxes to which they have access. Both the host computer and the remote sites can initiate data collection and distribution. A communications session with the Sterling Connect:Enterprise for UNIX repository can be initiated from an FTP or SSHFTP client, an Async or Bisync remote, a browser using the Sterling Connect:Enterprise HTTP, a Sterling B2B Integrator business process, or an AS2 trading partner. The following figures show the communications flow between the Sterling Connect:Enterprise for UNIX server installed in the trusted zone and its remote trading partners.



Sterling Connect:Enterprise for UNIX collects data files from remote sites for a central host site. For example, Sterling Connect:Enterprise can gather data generated by a database application for one remote site, then extract the data at the host site for use by a local application.

Sterling Connect:Enterprise for UNIX distributes data files from the host to one or more remote sites. The host site can automatically transmit output reports or data to remote sites. For example, if a company needs to send the latest sales report to its 25 regional sales offices, it can either send the report at a predetermined time to its sales offices or deposit the report in the repository and flag the report for transmission to the offices. The remote offices connect to the repository, obtain a listing of the repository contents, and request transmission of reports to their sites.

Sterling Connect:Enterprise for UNIX also enables you to schedule automated data collection and transmission between the host and an unattended remote site using the Auto Connect feature. You can schedule automated sessions by time of day, day of the week, day of the year, or you can initiate an Auto Connect session by issuing a host site operator command. An Auto Connect activity report is available after the Auto Connect session finishes.

## Sterling Connect:Enterprise for UNIX Terminology

The following table defines the concepts and terminology used with this product. The common synonym for a Sterling Connect:Enterprise for UNIX term is also specified.

<b>Term</b>	<b>Sterling Connect:Enterprise for UNIX Definition</b>	<b>Synonym</b>
Remote site	Remote terminal, application, or computer which is configured to initiate a communications session with the data repository.	Remote user, remote client
Host site	Sterling Connect:Enterprise for UNIX server on which the data repository resides.	server
Data repository	Entity that contains all mailboxes. It is similar to a file system, but no nesting is available.	Directory structure
Batch	Data file residing in a mailbox of the repository on the Sterling Connect:Enterprise host computer. When a batch is added to the repository, it is assigned a unique number (from 1 to 9,999,999).	File
Mailbox ID	<p>An identifier that defines the repository associated with a batch. Remote users access the contents of the VSAM batch files, where the batches are stored, using the Mailbox ID.</p> <p>A user can have access to a single mailbox (individual mailbox), a group mailbox (accessible by multiple users), and multiple mailboxes (accessible by a single user or trading partner).</p>	Directory
Batch ID (BID) or user batch ID	A description of the batch. It is also referred to as the user batch ID because it is assigned by the user. Multiple batches with the same batch ID can reside in a mailbox because each batch is given a unique batch number.	File name
Auto Connect	Unattended, scheduled communications session initiated by the Sterling Connect:Enterprise for UNIX repository to distribute or collect data.	
Remote connect	Communications session with the Sterling Connect:Enterprise for UNIX repository initiated by a remote site.	

---

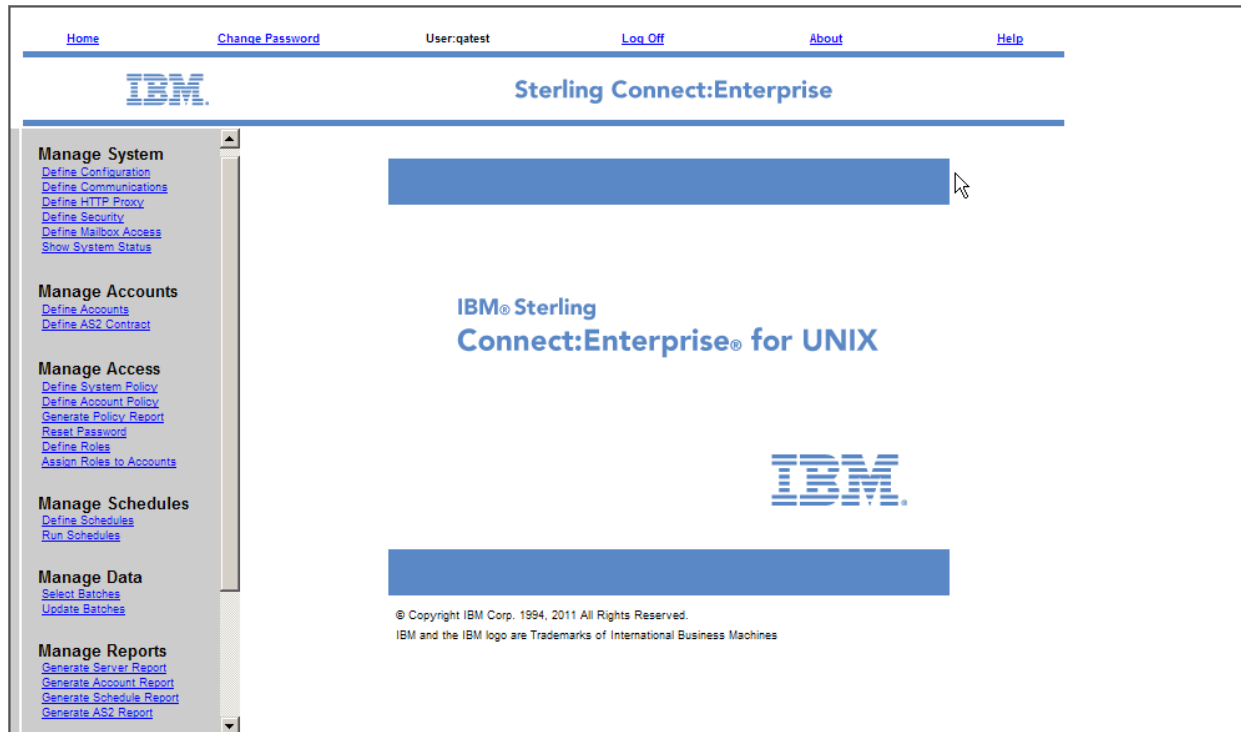
## Sterling Connect:Enterprise Features

Sterling Connect:Enterprise for UNIX has the following features:

- ◆ Firewall navigation support allows controlled access to a Sterling Connect:Enterprise system running behind a packet-filtering firewall without compromising your company security policies or those of your trading partner. Enhanced firewall navigation support provides the ability to limit ports used for FTP operations.
- ◆ Secure FTP with clear control channel (CCC) support enables clear text commands on the FTP control channel, allowing better interoperability with firewalls. The CCC command provides a way to negotiate the control connection from an encrypted content to a clear content. After the user ID and password have been transmitted in encrypted format, the remainder of the control channel communication is in clear text until the connection ends. All transmitted data remains encrypted.
- ◆ High availability support provides the capability to migrate an application from a failing system to another operational, or standby, system. In the event of a system failure, or fail over, the designated secondary system assumes control automatically with minimal or no loss of data. A system failure without high availability typically results in the loss of considerable time or data.
- ◆ Integration of communications and application services provides a reliable, seamless information flow across an organization and between customers and business partners, which reduces the need to integrate and re-integrate applications.
- ◆ Support for diverse operating environments, including support for multiple communications protocols such as AS2, FTP, Secure FTP, SSH through FTP and SCP, HTTP, asynchronous, bisynchronous, Sterling Connect:Direct, and Sterling B2B Integrator allows business processes to be shared with trading partners without dictating communications standards.
- ◆ Ability to deliver data to existing third-party applications, application servers, web servers and browsers, reduces the need to constantly integrate and re-integrate.
- ◆ Reporting that tracks enterprise-wide data movement provides a common view of data movement and file activity. Cereport is a reporting tool that provides end-to-end file and data movement reporting.
- ◆ The Sterling Connect:Enterprise File Agent tool monitors specified directories for files, then initiates processing of those files.
- ◆ MQSeries support allows data to be moved between the Sterling Connect:Enterprise repository and the IBM MQSeries product.
- ◆ The Sterling Connect:Enterprise Site Administration user interface allows you to administer Sterling Connect:Enterprise base from a browser.
- ◆ Role-based access allows you to specify sets of permissions and assign these permission sets to different users.

# Sterling Connect:Enterprise for UNIX Site Administration User Interface

The Sterling Connect:Enterprise for UNIX Administration user interface runs in a Web browser, as shown in the following screen.



The navigation bar on the left side of the screen provides access to the resources that you administer from the user interface. The following table describes the Sterling Connect:Enterprise resources.

Resource	Description
System	Enables you to define system configurations, communications protocol for AS2, FTP, async, and bisync connections, security parameters for Secure FTP, and permissions on a mailbox-by-mailbox basis. You can also view the status of batches during transmission.
Accounts	Enables you to define AS2 contracts and accounts for local and remote users who are authorized to access the Sterling Connect:Enterprise system.
Access	Enables you to define and assign roles for users of the Sterling Connect:Enterprise Site Administration interface, and create and assign password policies to users.

Resource	Description
LDAP	Enables you to configure the communications between Sterling Connect:Enterprise and the external authentication service and configure your server access definition for LDAP authentication.
Schedules	Enables you to define schedules for automatic transfers, add remote accounts to those schedules, and run schedules manually.
Data	Enables you to manipulate batches in the repository.
Reports	Enables you to generate reports on the server, accounts, schedules, and AS2 activity.

All users of the Sterling Connect:Enterprise for UNIX Site Administration user interface must be assigned a role. A role defines a set of permissions to perform specific tasks in each functional area. See Chapter 6, *Role-Based Access*, for information on designing and implementing a role-based access system for the Sterling Connect:Enterprise for UNIX Site Administration user interface. See also *Setting Up the Sterling Connect:Enterprise for UNIX Site Administration User Interface* on page 65 for instructions on configuring the Sterling Connect:Enterprise for UNIX Site Administration user interface.

## Sterling Connect:Enterprise Software

Sterling Connect:Enterprise software is distributed as follows, depending on whether you purchase Sterling Connect:Enterprise for UNIX with or without Secure FTP or AS2.

Component	Description	Installation Reference
Sterling Connect:Enterprise for UNIX Secure FTP or Sterling Connect:Enterprise for UNIX FTP	Provides the Sterling Connect:Enterprise for UNIX software with Secure FTP capability, AS2 capability, or without Secure FTP or AS2 capability, Sterling Connect:Enterprise File Agent.	<i>IBM Sterling Connect:Enterprise for UNIX Installation and Administration Guide</i> <i>IBM Sterling Connect:Enterprise Integration Tools User's Guide</i> (File Agent)
Sterling Connect:Enterprise for UNIX AS2		
IBM® Sterling Connect:Direct® for UNIX	Provides Sterling Connect:Direct for UNIX software.	<i>IBM Sterling Connect:Direct for UNIX Getting Started Guide</i>



Component	Description	Installation Reference
IBM® Sterling Connect:Direct® Browser User Interface	Enables you to create, submit, and monitor Sterling Connect:Direct Processes from an Internet browser and perform some Sterling Connect:Direct system administration tasks.	Sterling Connect:Direct Browser User Interface Readme file
IBM® Sterling Certificate Wizard	Packaged only with Sterling Connect:Enterprise for UNIX Secure FTP. Automates creating certificate signing requests.	Sterling Certificate Wizard ReadMe file

You can purchase the following components separately for use with Sterling Connect:Enterprise for UNIX:

Component	Description
IBM® Sterling Connect:Enterprise® Secure Client	A Java client that enables trading partners to send data to and receive data from a central Sterling Connect:Enterprise system using FTP, SSH, and WebDAV protocols.
IBM® Sterling Connect:Enterprise® Command Line Client (Secure FTP)	A command line client that enables trading partners to send data to and receive data from a central Sterling Connect:Enterprise system using FTP and SSH on both UNIX and Microsoft Windows platforms.
IBM® Sterling Connect:Direct® Secure Plus for UNIX	Provides enhanced security for Sterling Connect:Direct by using cryptography to secure data during transmission.
IBM® Sterling Connect:Enterprise® HTTP	Provides a Web interface that enables you to communicate with and request data from the Sterling Connect:Enterprise data repository over the Internet.

## Sterling Connect:Enterprise for UNIX Documentation

See *IBM Sterling Connect:Enterprise for UNIX Version 2.5.00 Release Notes* for a complete list of the product documentation.

### About This Guide

*IBM Sterling Connect:Enterprise for UNIX Installation and Administration Guide* is for programmers and network operations staff who install, configure, and maintain the Sterling Connect:Enterprise for UNIX version 2.5 product.

This guide assumes knowledge of the UNIX operating system, including its applications, network, and environment. If you are not familiar with the UNIX operating system, refer to the UNIX library of manuals.

## Task Overview

The following table directs you to the information required to perform the tasks documented in this guide:

<b>Task</b>	<b>For More Information, See</b>
Installing Sterling Connect:Enterprise for UNIX	Chapter 2, <i>Installing Sterling Connect:Enterprise for UNIX</i>
Installing Sterling Connect:Enterprise base	Chapter 2, <i>Installing Sterling Connect:Enterprise for UNIX</i>
Installing individual components of Sterling Connect:Enterprise for UNIX	Chapter 2, <i>Installing Sterling Connect:Enterprise for UNIX</i>
Upgrading from a previous version of Sterling Connect:Enterprise or Sterling Connect:Mailbox	Chapter 3, <i>Upgrading Sterling Connect:Enterprise for UNIX</i>
Exporting environment variables	Chapter 4, <i>Post-Installation Tasks</i>
Testing the installation	Chapter 4, <i>Post-Installation Tasks</i>
Setting up the Sterling Connect:Direct for UNIX Site Administration user interface	Chapter 4, <i>Post-Installation Tasks</i>
Starting and stopping Sterling Connect:Enterprise for UNIX	Chapter 5, <i>Starting and Stopping Sterling Connect:Enterprise</i>
Designing a role-based access system	Chapter 6, <i>Role-Based Access</i>
Defining and applying password policies, changing user password, and generating reports on RSD policy files	Chapter 7, <i>Password Administration</i>
Issuing administrator commands	Chapter 8, <i>Administrator Commands</i>
Generating reports	Chapter 9, <i>Generating Reports</i>
Installing Secure FTP	Chapter 10, <i>Configuring Secure FTP</i>
Implementing SSH FTP	Chapter 11, <i>Configuring SSHFTP Protocol</i>
Implementing AS2	Chapter 12, <i>Configuring AS2</i>
Implementing WebDAV	Chapter 13, <i>Configuring WebDAV Protocol</i>
Implementing External Authentication	Chapter 14, <i>Configuring the External Authentication Service</i>
Configuring Remote Daemons	Chapter 15, <i>Running Protocol Daemons on Remote Servers</i>

---

<b>Task</b>	<b>For More Information, See</b>
Implementing Sterling Connect:Enterprise in a high-availability environment	Chapter 16, <i>Configuring High Availability</i>
Implementing SIPS Encryption	Chapter 17, <i>Encrypting Internal Product Communications</i>
Troubleshooting problems	Appendix A, <i>Error Messages</i>

---



---

# Installing Sterling Connect:Enterprise for UNIX

This chapter provides information about the Sterling Connect:Enterprise for UNIX installation, describes preinstallation tasks, and details the steps for installing the system and its components.

The installation is divided into the following main procedures: starting the installation script, installing all Sterling Connect:Enterprise for UNIX components, installing Sterling Connect:Enterprise for UNIX base, installing Sterling Connect:Direct for UNIX, and configuring Sterling Connect:Enterprise for UNIX agents and cereport.

For instructions on upgrading from a previous version of Sterling Connect:Mailbox or Sterling Connect:Enterprise, refer to *Chapter 3, Upgrading Sterling Connect:Enterprise for UNIX*.

---

## Before You Begin

Perform the following tasks before you install Sterling Connect:Enterprise.

1. If you plan to use a third-party Web server to run the Sterling Connect:Enterprise Site Administration user interface, verify that you have installed and configured your Web server and servlet engine and that they are communicating with each other. By default, the Site Administration user interface runs on a Jetty web server that is installed with the product.
2. Read the *IBM Sterling Connect:Enterprise for UNIX Release Notes* completely. The release notes contain a list of software and hardware requirements and last-minute changes to the documentation.

3. Review your system and the descriptions of the installation options in the following table, and choose the installation to perform:

Installation Option	Description	Related Procedures
Install all components	<ul style="list-style-type: none"> <li>◆ Installs Sterling Connect:Enterprise for UNIX</li> <li>◆ Configures Secure FTP, SSH, High Availability, AS2, and HTTP server, as required for your system</li> <li>◆ Installs File Agent, MQ Agent, and cereport</li> </ul>	<ul style="list-style-type: none"> <li>◆ <i>Starting the Installation Script</i> on page 24</li> <li>◆ <i>Installing All Sterling Connect:Enterprise for UNIX Components</i> on page 25</li> <li>◆ <i>Installing Sterling Connect:Enterprise for UNIX Base</i> on page 26</li> </ul>
Install the base product	<ul style="list-style-type: none"> <li>◆ Installs Sterling Connect:Enterprise for UNIX</li> <li>◆ Configures SSH, Secure FTP, High Availability, AS2, and HTTP server, as required for your system</li> </ul>	<ul style="list-style-type: none"> <li>◆ <i>Starting the Installation Script</i> on page 24</li> <li>◆ <i>Installing Sterling Connect:Enterprise for UNIX Base</i> on page 26</li> </ul>
Upgrade the base product	Upgrades your installation from an earlier version of Sterling Connect:Mailbox or Sterling Connect:Enterprise	Refer to <i>Chapter 3, Upgrading Sterling Connect:Enterprise for UNIX</i> .
Install or upgrade remote daemons	Installs or upgrades a protocol daemon on a remote system such as a DMZ machine.	Refer to <i>Installing Sterling Connect:Enterprise Remote Daemons</i> on page 39.
Configure agents and cereport utility	Configures File Agent, MQ Agent, and cereport	<ul style="list-style-type: none"> <li>◆ <i>Starting the Installation Script</i> on page 24</li> <li>◆ <i>Configuring Sterling Connect:Enterprise File Agent, MQ Agent, and cereport</i> on page 42</li> </ul>

4. If you are installing or configuring any of the following components, refer to the associated chapter and complete the worksheet before starting the installation:

Component	Location of Worksheet
Secure FTP	<i>Configuring Secure FTP</i> on page 165
SSHFTP	<i>Configuring Sterling Connect:Enterprise SSH Server</i> on page 173
AS2	<i>Configuring Sterling Connect:Enterprise for UNIX for AS2</i> on page 181
High Availability	<i>Installing Sterling Connect:Enterprise High-Availability Scripts</i> on page 215

5. Create a user ID to use during installation. See the following *Creating the User ID* section.

6. Record the full path name of the directory in which you want Sterling Connect:Enterprise to reside.
7. Identify the port number for the Control daemon. This is the TCP/IP port number the Sterling Connect:Enterprise Control daemon monitors for connection requests from the other Sterling Connect:Enterprise daemons (the installation procedure provides a default value).
8. Identify the port number for the Service daemon. This is the TCP/IP port number the Sterling Connect:Enterprise Service daemon monitors for requests from the Sterling Connect:Enterprise Site Administration user interface (the installation procedure provides a default value).
9. Identify the FTP listener port. The port number should be 1024 or greater. If the port number is set to less than 1024, the user ID of *cmuftpd*, *ftp*, and *ftpd* must be set to root.
10. Identify whether your system will use Secure FTP communications, the sites that have Secure FTP capabilities, and record the host name and the cipher suites to use.

## Creating the User ID

You should create a unique user ID for use during installation, configuration, and maintenance. After installation is completed, this user ID is the owner of the Sterling Connect:Enterprise files.

To create a user ID, use the following steps:

1. Create a user ID called **ceuser** on the host UNIX workstation.  
This is the only ID that should have read/write/execute permission for the product binaries and the *\$CMUHOME/database* directories.
2. Log on to your UNIX environment as **ceuser**.

---

**WARNING:** Do not install Sterling Connect:Enterprise from the root account.

---

The Sterling Connect:Enterprise system administrator must use only one user ID to both install and run the product. If, for example, user *installer* installs the product and user *sysadmin* runs it, then file ownership permission conflicts can arise.

## Installation Script Conventions

The installation and configuration is performed with automated installation scripts. The following conventions are used in both installation and configuration scripts:

- ◆ Acceptable responses to prompts are indicated within brackets where Y or y means YES and N or n means NO.
- ◆ The default response is indicated within the bracketed choices as a capital letter. Press **Enter** to accept the default value.
- ◆ Do not use colons for values supplied at the prompts.
- ◆ Press **Ctrl+C** to terminate script execution.

---

## Starting the Installation Script

This section describes how to access the Sterling Connect:Enterprise for UNIX installation script, select the installation option, and specify the destination directory. You cannot install Sterling Connect:Enterprise for UNIX on networked storage media such as NFS or Samba shares.

1. Use one of the following methods for accessing the installation script:
  - ◆ If you acquired your Sterling Connect:Enterprise installation from an ESD portal, navigate to the location of the **ceinstall** script.
  - ◆ If you acquired your Sterling Connect:Enterprise installation on a CD-ROM, mount the Sterling Connect:Enterprise for UNIX CD-ROM.
2. At the UNIX prompt, type:

```
ceinstall
```

3. Press **Enter**. The following message is displayed:

```
=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX 2.5.00
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines

Installation Procedure

Please follow the Installation and Administration Guide and/or
Release Notes for the Sterling Connect:Enterprise component(s) to be installed.

UNIX(TM) is a registered trademark of The Open Group
=====
Press ENTER when ready.
```

4. Press **Enter**. The following message is displayed:

```
Enter the installation media location (mounted CD root, e.g. /cdrom/cdrom0/).
[/svshare/ceunix/2.5.00]:
```

5. Type the full path to the installation script or press **Enter** to accept the default. The installation menu is displayed.



```
Please select one of the following installation options:
```

- ```
(1) Install all Sterling Connect:Enterprise components
(2) Install or upgrade Sterling Connect:Enterprise base
(3) Install or upgrade Sterling Connect:Enterprise remote daemons
(4) Configure the Sterling Connect:Enterprise agents and cereport
(5) EXIT
```

```
Enter your choice:[1]
```

6. Refer to one of the following procedures, depending on the type installation you are performing:
  - ◆ *Installing All Sterling Connect:Enterprise for UNIX Components* on page 25
  - ◆ *Installing Sterling Connect:Enterprise for UNIX Base* on page 26
  - ◆ *Installing Sterling Connect:Enterprise Remote Daemons* on page 39
  - ◆ *Configuring Sterling Connect:Enterprise File Agent, MQ Agent, and cereport* on page 42

---

## Installing All Sterling Connect:Enterprise for UNIX Components

To install all Sterling Connect:Enterprise for UNIX components (File Agent, MQ Agent, and cereport), use the following procedure. To install Sterling Connect:Direct for UNIX, use the Sterling Connect:Direct for UNIX installation media and refer to the *IBM Sterling Connect:Direct for UNIX Getting Started Guide*:

1. Complete the procedure in *Starting the Installation Script* on page 24.
2. When the Installation menu is displayed, type **1** and press **Enter**. The following message is displayed:

```
Sterling Connect:Enterprise will be installed in your system. Do you want to
continue?: [Y/n]
```

3. Press **Enter**. The following message is displayed:

```
Enter the FULL path of the destination directory into which to install IBM(R)
Sterling Connect:Enterprise(R) for UNIX 2.5.00.
You can use $HOME/ceunix to shorten the name: [$HOME/ceunix]
```

4. Type the complete path to the directory where you want to install Sterling Connect:Enterprise for UNIX and press **Enter**.

---

**Note:** To get maximum capacity for your mailbox repository, the fully qualified path of your installation directory should be 31 characters or less.

Do not use a dash (-) in the path of the destination directory.

---

The following message is displayed:

```
You have chosen /installdirectory
as the destination directory. Please confirm: [Y/n]
```

5. Press **Enter** to confirm the destination directory.
6. Complete the procedure outlined in *Installing Sterling Connect:Enterprise for UNIX Base* on page 26.

---

## Installing Sterling Connect:Enterprise for UNIX Base

To install Sterling Connect:Enterprise for UNIX base only, use the following procedure.

1. Complete the procedure in *Starting the Installation Script* on page 24.
2. Type **2** to specify the installation and press **Enter**. The following message is displayed:

```
Sterling Connect:Enterprise base Version 2.5.00 will be installed in your system.
Do you want to continue?: [Y/n]
```

3. Press **Enter**. The following message is displayed:

```
Enter the FULL path of the destination directory into which to install IBM(R)
Sterling Connect:Enterprise(R) for UNIX 2.5.00.
You can use $HOME/ceunix to shorten the name: [$HOME/ceunix]
```

4. Type the complete path to the directory where you want to install Sterling Connect:Enterprise for UNIX or accept the default and press **Enter**.

---

**Note:** To get maximum capacity for your mailbox repository, the fully qualified path of your installation directory should be 31 characters or less.

Do not use a dash (-) in the path of the destination directory.

---

The following message is displayed:

```
You have chosen /installdirectory
as the destination directory. Please confirm: [Y/n]
```

5. Press **Enter**. The following message is displayed:

```

=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines
version 2.5.00 Installation Procedure

You are beginning the Sterling Connect:Enterprise Installation Procedure.
You have specified the following directory (called the destination directory)
/data/ceu2500_base
where the Sterling Connect:Enterprise files will be stored.

After the files are extracted from the media, a customization procedure
will be called. It will configure the Sterling Connect:Enterprise operating
environment for you.

UNIX(TM) is a trademark of X/Open Company, Ltd. in the U.S.A and other
countries.
=====

Press ENTER when ready.

```

6. Press **Enter**. The following prompt is displayed:

```

**Please insert the media if you have not done so already.

Press Enter when ready.

```

7. Press **Enter**. A prompt similar to the following is displayed:

```

Installing Sterling Connect:Enterprise ...

Approximately 250000 kbytes of disk space is required
to install Sterling Connect:Enterprise.
(Some of this space is needed for temporary files required to do the install)

=====
Here is the current free disk space for each disk partition:
=====

Filesystem      1024-blocks      Free %Used      Iused %Iused Mounted on
/dev/hd4         393216           154208  61%      10850  21% /
/dev/hd2         2752512          375808  87%      51605  36% /usr
/dev/hd9var      524288           157020  71%      9952   21% /var
/dev/hd3         262144           255796  3%        302    1% /tmp
/dev/hd11admin   131072           130692  1%         5     1% /admin
/proc            -                 -      -         -     - /proc
/dev/hd10opt     524288           311100  41%      8762  11% /opt
/dev/livedump    262144           261776  1%         4     1% /var/adm/ras/livedump
/dev/fslv00     102760448        65773840 36%     142143  1% /data

You have ##### kbytes of disk space available to you,
which is more than the required 250000 kbytes.

Do you want to continue? [Y/n]

```

8. Press **Enter** to continue if the disk space is sufficient. Sterling Connect:Enterprise extracts all the files required for installation. The name of each extracted file is listed on the screen. The following screen is displayed:

```
Press ENTER to start the customization process.
```

9. Press **Enter** to continue the installation and customize Sterling Connect:Enterprise. The following screen is displayed:

```

=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines
version 2.5.00 Customization

The customization procedure sets up the Sterling Connect:Enterprise
operating environment. Help can be obtained from any prompt by entering (?)
followed by ENTER. To abort the process, enter Control-C.

As a shorthand, entering ENTER at the prompt means the default value, if any.
=====

Press ENTER when ready.

The core daemons will run on the local host (in the case of
a standalone installation), or will run using a shared
hostname (in the case of a High Availability or clustered
installation).

Please enter the correct system hostname : [server01] You entered server01. Is
this correct? [Y|n]
```

10. Type the system host name or accept the default and press **Enter** to begin the customization procedure to create the Sterling Connect:Enterprise system.
11. When you are prompted, confirm the host name and press **Enter**. The following message is displayed:

```

....Creating MCD file....

....Get MED file parameters....

....Creating sample shell profiles (kshrc, cshrc and profile) in
/data/ceu2500_base/etc/ ....

We strongly recommend using a port value > 1023. A lower port value
requires that all Sterling Connect:Enterprise daemons run with setuid root.

Enter port number for the Control daemon listener: [8000]
```

12. Type the TCP/IP port number that the Sterling Connect:Enterprise Control daemon monitors for connection requests from other Sterling Connect:Enterprise daemons, or press **Enter** to accept the default.

```
Enter port number for the Web Services daemon listener: [8001]
```

13. Type the TCP/IP port number that the Sterling Connect:Enterprise Web Services daemon monitors for connection requests from the Sterling Connect:Enterprise Site Administration user interface, or press **Enter** to accept the default.

```

...Creating C shell 'cshrc' file...

...Creating Korn shell 'kshrc' file...

...Creating Bourne shell 'profile' file...

...Creating ftp.cpd file...

We recommend using a port value > 1023.  A lower port value requires
that the FTP daemons run with setuid root.

Enter FTP listener port number: [10021]

```

14. Type the TCP/IP port number that the Sterling Connect:Enterprise FTP daemon monitors for connection requests from remote sites, or press **Enter** to accept the default.

```

Creating / Updating Roles Database ...

Successfully created data files and indices

Roles database: Complete.

Do you want this userid [user] to run the product and administer the Web Admin
Tool? [Y|n]

```

15. Specify whether you want the user ID that is performing the installation to perform vital functions to Sterling Connect:Enterprise. If you select n and press Enter, the userID that is installing the product cannot perform vital functions to Sterling Connect:Enterprise.

If you type y and press **Enter**, You are prompted with the following:

```

Creating Remote Site Definition (RSD) file for [user]
Please enter the Sterling Connect:Enterprise for UNIX RSD password [user]:

```

16. Type the password associated with userID and press **Enter**. The following messages are displayed:

```

Please enter the Sterling Connect:Enterprise RSD password [user]:
Giving administrative privileges to RSD [user]

The administrator roles and accounts were created successfully.

```

---

## Customizing Sterling Connect:Enterprise for UNIX

Based on the supplemental components you purchase, you can customize Sterling Connect:Enterprise for UNIX for the following options:

- ◆ Secure FTP
- ◆ SSH
- ◆ High availability
- ◆ AS2
- ◆ HTTP server (WebDAV)

The customization script prompts you to configure these options. Supply the information requested for each option you want to configure.

Before you configure and install these components, refer to the associated chapter listed in the following table and complete the worksheet before starting the installation:

| Component         | Location of Worksheet                                                                        |
|-------------------|----------------------------------------------------------------------------------------------|
| Secure FTP        | <i>Configuring Secure FTP</i> on page 165                                                    |
| SSHFTP            | <i>Configuring Sterling Connect:Enterprise SSH Server</i> on page 173                        |
| AS2               | <i>Configuring Sterling Connect:Enterprise for UNIX for AS2</i> on page 181                  |
| High Availability | <i>Installing Sterling Connect:Enterprise High-Availability Scripts</i> on page 215          |
| HTTP (WebDAV)     | For more information on configuring WebDAV, see the Site Administration User Interface Help. |

### Setting Up Secure FTP

If you have Sterling Connect:Enterprise Secure FTP, the customization script displays the following prompt:

```
Some protocols provided by this product may require X.509 certificates.
You can generate a Certificate Signing Request (CSR) and verify
keycert files with the Certificate Wizard shipped with this
product on a separate CD_ROM.

Do you want to configure for SSL? [Y|n]
```

---

**Note:** If you do not want to set up Secure FTP at this time, type **n** and press **Enter**. You can set up Secure FTP at a later time using the *\$CMUHOME/etc cmusslcust* script.

---

1. To set up Secure FTP, press **Enter**. The following prompt is displayed:

```

** Sterling Connect:Enterprise Secure FTP with SSL Setup Script
**
**
Doing FTP with SSL requires private key and certificate pair(s).
Now creating a ssl.spd Security Protocol Definition file
for production use.

You must use the Certificate Wizard or equivalent to generate
a private key and Certificate Signing Request (CSR) to obtain
a certificate from a Certificate Authority (CA), such as
Verisign or Thawte.

When complete, place the concatenated private key and cert
in the /data/ceu2500_base/spd/keycert.txt file.
Add the trusted root certificate from the CA to the
/data/ceu2500_base/spd/trusted.txt file.

Enter the Security Policy you would like for your FTP connections
(1=REQUIRED, 2=OPTIONAL, 3=DISALLOWED): [2]

```

2. Type the number corresponding to the level of security you want to implement. If you have not installed your certificate, select **3=DISALLOWED**. After you install your certificate, change your setting to enable Secure FTP in the **Security Policy** field of your SPD file(s).

If you select **1=REQUIRED** or **2=OPTIONAL**, the following screen is displayed:

```

Enter the Cipher Strength you would like for your FTP connections
(1=STRONG, 2=EXPORT, 3=ALL): [3]

```

3. Type the number corresponding to the appropriate cipher strength for the sites with which you exchange data. See Chapter 10, *Configuring Secure FTP*, for more information regarding cipher suites.

```

SPD file /data/ceu2500_base/spd/ssl.spd has been created.

Adding /data/ceu2500_base/spd/ssl.spd as the default spd file in
/data/ceu2500_base/cpd/ftp.cpd
**
**
Sterling Connect:Enterprise provides a CEU Factory Keycert / Cert pair
for testing purposes.

The CEU Factory Keycert pair may be used for FTP or AS2
SSL/TLS sessions.
The keycert may be used for AS2 payload signing and decryption.
The cert may be used for AS2 signature verification and encryption.

DO NOT USE THE CEU FACTORY KEYCERT FOR PRODUCTION!

SPD file /data/ceu2500_base/spd/CEUFactoryKeycert.spd has been created.
Press ENTER to continue.

```

Press **Enter** to continue.

The information you entered for the Secure FTP script is set in the default SPD file, `ssl.spd`. The `ssl.spd` file is then set as the default **Security protocol file** in `ftp.cpd`. Refer to and Chapter 10, *Configuring Secure FTP*, for more information.

## Setting Up SSH

You are prompted to setup SSH.

```
Do you want to configure for SSH [Y|n]
```

---

**Note:** If you do not want to set up SSH at this time, type **n** and press **Enter**. You can set up SSH at a later time using the `$CMUHOME/etc cmusscust` script.

---

1. Press **Enter**. The following prompt is displayed:

```
Enter SSHFTP listener port number : [10022]
```

2. Type the TCP/IP port number that the Sterling Connect:Enterprise SSHFTP daemon monitors for remote connection requests or press **Enter** to accept the default. One of the following prompts are displayed:

- ◆ If a supported source of random data is not available on your system, the following is displayed:

```
Creating SSH file sshftp.cpd
Checking for supported sources of random data.
RAND_status [0]
A random source has not been found.

Select one of the following options for gathering entropy.

1. Use entropy commands. (Default)
2. Use a named pipe.
3. Use a local port.

Enter option number to select entropy randomness routine:
```

- ◆ If a supported source of random data is available on your system, the following is displayed:

```
Creating SSH file sshftp.cpd
Checking for supported sources of random data.
RAND_status [1]
A random source has been found and is seeded.

A supported random source will be used for gathering entropy.
For better randomness, specify one of the following options,
or just press ENTER to only use the random source.

1. Use a named pipe.
2. Use a local port.
3. Use entropy commands.

Enter option number to select additional randomness:
```

3. Type the option number for additional randomness, or accept the default (if a supported source of random data was found, the default is none) and press **Enter**. The following prompt is displayed:



```

Creating entropy environment variables.
Creating SSH files ssh_host_key and ssh_host_key.pub
Enter type of host key to create, rsa or dsa: [rsa]

```

4. Specify to use an RSA or DSA host key and press **Enter**. The following prompt is displayed:

```
Specify number of bits in the key (512 - 32768) to create: [1024]
```

5. Specify the number of bits to use in the host key and press **Enter**. Valid values are 512–32768. However, some clients and servers cannot handle keys larger than 2048 bits. The following prompt is displayed:

```
Enter passphrase (press return for no passphrase):
```

6. Type the passphrase to use for the host key or leave blank for no passphrase and press **Enter**. The following prompt is displayed:

```
Enter same passphrase again:
```

7. Type the same passphrase to confirm and press **Enter**. The following prompt is displayed:

```

cmusshkey: ssh host key generation and maintenance utility
Generating public/private rsa host key pair.
Your private key is being saved in:
 /data/ceu2500_base/ssh/system/ssh_host_key
Your public key is being saved in:
 /data/ceu2500_base/ssh/system/host_key.pub
The public key fingerprint is:
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx user01@hostname
cmusshkey: ending successful.

Press ENTER to continue.

```

8. You can specify to create a keypair for samp\_ssh, the sample available for testing SSH. Do one of the following: If you do not want to create this key pair, type **n** and press **Enter** and Refer to *Configuring High Availability* on page 34. To build this key pair, do the following:

- a. Type **Y** press **Enter**. The following prompt is displayed:

```
Enter passphrase (press return for no passphrase):
```

- b. Type **Y** or leave blank for no passphrase and press **Enter**. The following prompt is displayed.

```
Enter same passphrase again:
```

- c. Type the same passphrase again and press **Enter**. The following prompt is displayed:

```

cmusshkey: ssh host key generation and maintenance utility
Generating public/private rsa host key pair.
Your private key is being saved in:
  /data/ceu2500_base/ssh/users/samp_ssh/id_rsa
Your public key is being saved in:
  /data/ceu2500_base/ssh/users/samp_ssh/id_rsa.pub
The public key fingerprint is:
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx user01@hostname
cmusshkey: ending successful.
-----
Press ENTER to continue.

```

## Configuring High Availability

You are prompted to configure high availability.

```
Do you want to configure High Availability [y|N]
```

---

**Note:** If you do not want to set up high-availability at this time, press **Enter**. Refer to Chapter 16, *Configuring High Availability*, for information on configuring high availability at a time other than initial installation.

---

1. Type **y** and press **Enter**. The high-availability scripts and configuration files are modified to have host-specific values.
2. When you are prompted for the correct location of the destination directory, you can accept the default or type **n** and specify the correct path.

```

The following directory (called the destination directory):
  /host/users/user01/ceunix25
was detected to be the location of Sterling Connect:Enterprise Secure FTP.

Is this correct? [Y|n]

```

The script continues and verifies that all files are in the correct location. CMUHOME, CMUSER, and CMUPORT are replaced with appropriate values throughout the high-availability configuration files, and the script then prints the following message:

```

=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
Version n.n High-Availability Package Installation Procedure

The Sterling Connect:Enterprise for UNIX High-Availability Package
Installation Procedure is complete. You must now register the
High Availability package with the Package Manager. Please
reference the appropriate instructions in the Sterling Connect:Enterprise for
UNIX High-Availability Package Installation Guide.
=====
Press Enter...

```

## Setting Up AS2

You are prompted to configure AS2.

```
Do you want to configure AS2 [y|N]
```

---

**Note:** If you do not want to set up AS2 at this time, press **Enter**. You can set up AS2 at a later time using the `$CMUHOME/etc as2cust` script.

---

1. Type **y** and press **Enter**. You are prompted as follows:

```
=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines
version 2.5.00 Customization

This customization procedure sets up AS2 for IBM(R) Sterling
Connect:Enterprise(R) for UNIX
operating environment.

As a shorthand, entering ENTER at the prompt means use the default value, if any.
To abort the process, enter Control-C.
=====

Press ENTER when ready.
```

2. Press **Enter** to continue. You are prompted as follows:

```
Using Java Runtime "/data/ceu2500_base/jre/bin/java"

Created script: /data/ceu2500_base/javaliib/cmuhttpd
Created script: /data/ceu2500_base/javaliib/cmuediintd
Created script: /data/ceu2500_base/javaliib/as2report
Created script: /data/ceu2500_base/javaliib/as2delete

Enter a name for the AS2 Port [port1]:
```

3. Type a name for the AS2 port and press **Enter**. You are prompted as follows:

```
We strongly recommend using a port value > 1023. A lower port value
requires that all daemons run with setuid root.
Enter port number for the AS2 listening port: [9000]
```

4. Type a port number for the AS2 port (greater than 1023 recommended) and press **Enter**. You are prompted as follows:

```
Enter a name for the Dead-letter mailbox [deadmbx]:
Created: /data/ceu2500_base/as2/AS2-Configuration.xml

AS2 Customization Completed
```

5. Type a name for the dead-letter mailbox and press **Enter**. The following messages are displayed:

```
Created: /data/ceu2500_base/as2/AS2-Configuration.xml

AS2 Customization Completed
Initializing Databases and Creating Admin Role

Creating Mailbox Database
Date: 02/28/11          IBM Sterling Connect:Enterprise for UNIX          Page: 1
Time: 14:25:09          Initialize Mailbox

Mailbox Name: cmumbox
Processing Status: Successful Initialization
Mailbox Database initialized
```

## Setting Up the HTTP Server

Sterling Connect:Enterprise for UNIX includes an HTTP Web server to support the Site Administration user interface. This is an alternative to using a third-party Web server.

You are prompted to configure the HTTP server.

```
Would you like to install the HTTP Server? This includes DAV support if licensed.
[Y|n]
```

---

**Note:** If you do not want to set up the HTTP server at this time, press **Enter**. You can set up the HTTP server at a later time using the `$CMUHOME/etc as2cust` script as follows:

```
as2cust admin port host
```

where *port* is the port number that cmusvid is monitoring and *host* is the host that cmusvid is running on.

---

1. To configure the HTTP Web server, type **y** and press **Enter**. The following prompt is displayed:

```
Using Java Runtime "/data/ceu2500_base/jre/bin/java"

Created script: /data/ceu2500_base/javailib/cmoadmind

Enter a name for the admin Port [admin]:
```

2. Type a name for the admin port and press **Enter**. The following prompt is displayed:

```
We strongly recommend using a port value > 1023. A lower port value
requires that all daemons run with setuid root.
Enter port number for the admin listening port: [9001]
```

3. Type the port number for the HTTP Services daemon listener that the Web server will use to accept requests from the Site Administration user interface or accept the default and press **Enter**. The following prompt is displayed:

```
Created: /data/ceu2500_base/cpd/admin/Admind.xml

After starting the system, you can open your browser to:
  http://hostname:9001/ceuadmin/jsp/index.jsp for web admin
to start the web browser interface.

For webDAV access use:
  http://hostname:port#/ceudav/

Press ENTER to continue.
```

---

## Completing the Installation

After all components are configured, the script continues with the following messages:

```

....Creating ceustartup script....

....Creating ceustartup.trace script....

....Creating ceushutdown script....

=====
Sterling Connect:Enterprise configuration completed.

----- NOTE -----
Before using Sterling Connect:Enterprise, please export the following
Sterling Connect:Enterprise environment variables.

export CMUHOME=/data/ceu2500_base
export CMUHOST=hostname
export CMUPORT=8000
export PATH=$PATH:$CMUHOME/etc:$CMUHOME/aix/bin:$CMUHOME/javali
export LD_LIBRARY_PATH=$CMUHOME/aix/lib
export LIBPATH=$CMUHOME/aix/lib
export SHLIB_PATH=$CMUHOME/aix/lib

You can set the environment variables by executing
. /data/ceu2500_base/etc/profile
at the shell prompt

OR

incorporate $CMUHOME/etc/profile
into your environment.

=====

Please press ENTER to continue...

```

1. Press **Enter** to complete the installation. The following prompt is displayed:

```

=====
Sterling Connect:Enterprise configuration completed.

To bring up the Sterling Connect:Enterprise system, at the shell prompt
run ceustartup.

To bring down the Sterling Connect:Enterprise system, at the shell prompt
run ceushutdown.
=====

IBM(R) Sterling Connect:Enterprise(R) for UNIX version 2.5.00 install successful.

Would you like to return to the Sterling Connect:Enterprise
installation menu? [Y|n]

```

2. To return to the Sterling Connect:Enterprise for UNIX installation menu, press **Enter**. If you completed the installation, type **n** and press **Enter**. A command prompt is displayed.

---

## Installing Sterling Connect:Enterprise Remote Daemons

Sterling Connect:Enterprise for UNIX supports the ability to run protocol daemons on a system other than where the base product is installed, such as a system in the DMZ. After installing the base product on the host system, use the following procedure on the target remote system to install the protocol daemons.

1. Complete the procedure in *Starting the Installation Script* on page 24.
2. With the Installation menu displayed, type **3**, and press **Enter**. The following prompt is displayed:

```
This is the IBM(R) Sterling Connect:Enterprise(R) for UNIX Remote Daemon
installation process.

Selected Sterling Connect:Enterprise 2.5.00 protocol daemons will be
installed on this host.  If you want to install these daemons on
another server, take the media to that server and run this
installation there. Do you want to continue with this installation? [Y|n]
```

3. Press **Enter**. The following prompt is displayed:

```
Enter the FULL path of the destination directory into which to install IBM(R)
Sterling Connect:Enterprise(R) for UNIX 2.5.00.
You can use $HOME/ceunix to shorten the name: [/data/users/user/ceunix]
```

4. Type the host name where you want to install the daemons and press **Enter**. The following prompt is displayed:

```
You have chosen /data/hostname
as the destination directory. Please confirm: [Y|n]
```

5. Press **Enter** to continue. The following prompt is displayed.

```
Installing from /svshare/ceunix/2.5.00/Base/cebase2500s.cpio.

** Please insert the media if you have not already done so.

Press ENTER when ready.
```

6. Press **Enter** to continue. The following prompt is displayed:

```

Installing Sterling Connect:Enterprise 2.5.00

Approximately 150000 kbytes of disk space are required
to install the Sterling Connect:Enterprise remote daemons.
(Some of this space is needed for temporary files required to do the install)

=====
  Here is the current free disk space for each disk partition:
=====

Filesystem      1024-blocks      Free %Used      Iused %Iused Mounted on
/dev/hd4         393216           153984  61%           10850  21% /
/dev/hd2         2752512          375808  87%           51605  36% /usr
/dev/hd9var      524288           156996  71%            9952  21% /var
/dev/hd3         262144           255800   3%             300   1% /tmp
/dev/hd11admin   131072           130692   1%              5   1% /admin
/proc            -                -         -              -   - /proc
/dev/hd10opt     524288           311100  41%            8762  11% /opt
/dev/livedump    262144           261776   1%              4   1% /var/adm/ras/livedump
/dev/fslv00     102760448        65434700 37%          144665   1% /data

You have 65434700 kbytes of disk space available to you,
which is more than the required 150000 kbytes.

Do you want to continue? [Y|n]

```

7. Press **Enter** to continue. After the binaries are installed, the following prompt is displayed:

```

=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines

Version 2.5.00 Remote Daemon Customization

The customization procedure sets up the Sterling Connect:Enterprise Remote Daemon
operating environment. Help can be obtained from any prompt by entering (?)
followed by ENTER. To abort the process, enter Control-C.

As a shorthand, entering ENTER at the prompt means the default value, if any.
=====

Press ENTER when ready.

```

8. Press **Enter** to continue. The following prompt is displayed:

```

Please enter the system hostname where core daemons are running : [remoteserver]

```

9. Type the name of the host where the Sterling Connect:Enterprise server is running and press **Enter**.

---

**Note:** Do not accept the default. It is the name of the remote server. You need to type the name of the server where the Sterling Connect:Enterprise core daemons are running.

---



The following prompt is displayed:

```
You entered cehost. Is this correct? [Y|n]
```

10. Verify the host name and press **Enter**. The following prompt is displayed:

```
Enter port number for the Control daemon listener on the core machine: [8000]
```

11. Type the port number of the control daemon that resides on the host specified in step 9 on page 40 and press **Enter**.
12. The following prompt is displayed:

```
....Creating sample shell profiles (kshrc, cshrc and profile) in
/data/ceu2500_remotes/etc/ ....

....Creating C shell 'cshrc' file....

....Creating Korn shell 'kshrc' file....

....Creating Bourne shell 'profile' file....

Do you want to configure for FTP? [Y|n]
```

13. To install the FTP daemon on the remote server, type **y** and press **Enter**. The following prompt is displayed:

```
We recommend using a port value > 1023. A lower port value requires
that the FTP daemons run with setuid root.

Enter FTP listener port number: [10021]
```

14. Type the listener port number of the FTP daemon and press **Enter**. If you have Sterling Connect:Enterprise Secure FTP, the The following prompt is displayed:

```
Some protocols provided by this product may require X.509 certificates.
You can generate a Certificate Signing Request (CSR) and verify
keycert files with the Certificate Wizard shipped with this
product on a separate CD_ROM.

Do you want to configure for SSL? [Y|n]
```

15. If want to set up SSL, type **y** and press **Enter**. Refer to *Setting Up Secure FTP* on page 30.
16. After you set up SSL, the following prompt is displayed:

```
Do you want to configure for SSH? [Y|n]
```

17. To install the SSH daemon on the remote server, type **y** and press **Enter**. Refer to *Setting Up SSH* on page 32 for information on setting up SSH. After you set up SSH, The following prompt is displayed:

```
Do you want to configure for AS2? [y|N]
```

18. If want to set up the AS2 HTTP daemon, type **y** and press **Enter**. Refer to *Setting Up AS2* on page 35. After you set up the AS2 HTTP daemon, The following prompt is displayed:

```
Sterling Connect:Enterprise supports a web-based Admin GUI.  
Would you like to install the Admin GUI? This includes DAV support if licensed. [Y|n]
```

19. To install the HTTP daemon to serve WebDAV requests, type **y** and press **Enter**. Refer to *Setting Up the HTTP Server* on page 36 for information on setting up the HTTP daemon. After you set up the HTTP daemon, refer to *Completing the Installation* on page 37.
20. Refer to *Running Protocol Daemons on Remote Servers* on page 205 for additional information.

---

## Installing Sterling Connect:Direct for UNIX

To install Sterling Connect:Direct for UNIX, use the Sterling Connect:Direct for UNIX installation media and refer to the *IBM Sterling Connect:Direct for UNIX Getting Started Guide*.

---

## Configuring Sterling Connect:Enterprise File Agent, MQ Agent, and cereport

To configure MQ Agent and cereport:

1. Complete the procedure in *Starting the Installation Script* on page 24.
2. With the Installation menu displayed, type **4**, and press **Enter**. The following prompt is displayed:

```
Sterling Connect:Enterprise 2.5.00 agents and cereport will be  
configured for your system. Do you want to continue? [Y|n]
```

3. Type **y** and press **Enter**. The following prompt is displayed:

```
Please enter Sterling Connect:Enterprise home directory [/data/ceu2500]:
```

4. Type the home directory or accept the default and press **Enter**.

## Configuring File Agent

1. The installation program displays the following prompt:

```
Do you want to configure the file agent at this time? [y/N]:
```

2. Type **y** and press **Enter**, which displays the following prompt.

```
Enter Sterling Connect;Enterprise UNIX API connection information below.  
Enter Sterling Connect:Enterprise for UNIX Host [localhost]:
```

3. Type the host server name where File Agent resides and press **Enter**. The default is the value of the \$CMUHOST environment variable if it is available in the shell where the install script is started. The following prompt is displayed:

```
Enter Sterling Connect:Enterprise API port number [8000]:
```

4. Type the API port number that corresponds to the control port number entered during the Sterling Connect:Enterprise installation and press **Enter**. The default is the value of the \$CMUPORT environment variable if it is available in the shell where the install script is started. The following prompt is displayed:

```
Enter Sterling Connect:Enterprise API RemoteID [username]:
```

5. Type the Sterling Connect:Enterprise API remote ID and press **Enter**. This is the Sterling Connect:Enterprise user ID that the File Agent uses as the originating mailbox remote for all batches added to Sterling Connect:Enterprise through the File Agent. The default is the value of either the LOGON or USER environment variables if they are available in the shell where the install script was started. The following prompt is displayed:

```
Enter Sterling Connect:Enterprise API Password [username]:
```

6. Type the Sterling Connect:Enterprise API password that corresponds to the remote ID and press **Enter**. The default is the value of the remote ID.

---

**Note:** Set the remote ID and the password values to match the Sterling Connect:Enterprise superuser ID. This is the administrative ID used by the administrator for Sterling Connect:Enterprise. This prevents internal security in Sterling Connect:Enterprise from interfering with the operation of the File Agent.

---

The following prompt is displayed.

```
Warning: The Sterling Connect:Enterprise password you entered will be written to
the disk in plain text. This can compromise your system's security. A more secure
option is to have the file agent prompt for the password at each startup. To
continue with the current operation reenter the password below. To have the File
Agent prompt for the password at startup, simply press Enter.
```

7. To accept the password risk, retype the password and press **Enter** or press **Enter** to require file agent to prompt for a password. The following prompt is displayed:

```
Sterling Connect:Enterprise for UNIX API Host:           hostname
Sterling Connect:Enterprise for UNIX API Port:          portnumber
Sterling Connect:Enterprise for UNIX API User Name:     user01
Sterling Connect:Enterprise for UNIX API User Password: password
Confirm the above values are correct. [Y|n]:
```

8. Press **Enter** to accept the values. The following prompt is displayed:

```
Enter the wait cycles [2]:
```

9. Type the number of wait cycles or accept the default and press **Enter**. The wait cycle defines the number of times a file is checked to ensure that the file is completed. The following prompt is displayed:

```
Enter the interval in seconds [15]:
```

10. Type the interval in seconds and press **Enter**. This specifies the amount of time between each check. The total time that a file must remain unmodified to be processed by the File Agent is calculated as wait cycles times interval. For example, if interval is 15 and wait cycle is 4, the file must be idle for a total of at least 60 seconds and a maximum of 75 seconds before processing begins. The following prompt is displayed:

```
Enter the subprocess limit (1-20) [2]:
```

11. Type the subprocess limit and press **Enter**. This is the number of concurrent UNIX child processes that can run at one time. The default is 2. The following prompt is displayed:

```
Cycles:                #
Interval:              ##
Subprocess limit:      ##
Sterling Connect:Enterprise for UNIX API Host:           hostname
Sterling Connect:Enterprise for UNIX API Port:          portnumber
Sterling Connect:Enterprise for UNIX API User Name:     username
Sterling Connect:Enterprise for UNIX API User Password: password
Are these values correct. [Y|n]:
```

12. Carefully inspect the values. This is the last time you can change them during installation. If these values are correct, type **y** and press **Enter** to accept the values.

If one or more values are incorrect:

- a. Type **n** and press **Enter**.
- b. Press **Enter** to move through the list of values until you find the one to change.

- c. Type in the new value. Press **Enter** until you are prompted to verify the File Agent configuration values.
- d. Carefully inspect the values. This is the last time you can change them during installation.
- e. Type **y** and press **Enter** to accept the values specified.

The following prompt is displayed:

```
Configuration of File Agent is complete.

Press Enter to continue.
```

## Configuring MQ Agent

The customization script continues with the following prompt.

```
The Sterling Connect:Enterprise Agent Configuration Script can configure
the MQ Series agents at this time. You will need to have the
MQ Series libraries installed on your system in order to use the
MQ Series agents.

If you do not have the MQ Series libraries installed now, you should
choose 'no' at the prompt, install the libraries, and run
'ceuagtcust' at a later time in order to set up the MQ Series agents.

If you do have the MQ Series libraries installed now, you may
choose 'yes' at the prompt in order to set up the MQ Series agents.

Do you want to configure MQ Series at this time? [y|N]:
```

---

**Note:** If you do not want to set up MQ series agents at this time, type **n** and press **Enter**. You can set up MQ series agents at a later time using the `$CMUHOME/etc ceuagtcust` script.

---

1. If you have the necessary libraries, type **y** and press **Enter**. You are prompted with the following:

```
Sterling Connect:Enterprise Agent Customization script has completed.

Press Enter to continue.
```

2. The following prompt is displayed. To configure cereport, type **y** and press **Enter**.

```
Do you you want to configure cereport at this time?: [N|y]
```

## Configuring cereport

The customization script continues with the following prompt.

```
=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines

cereport Customization.

The customization procedure will create or override cereport script in
directory /data/ceu2500/etc.

To abort the process, enter Control-C.

=====

Please press ENTER to continue...
```

1. Press **Enter**. The following is displayed:

```
Using Java Runtime "/data/ceu2500/jre/bin/java" to configure CeReport

Enter the FULL path name of the Sterling Connect:Direct
log directory: []
```

2. Type the directory to use for Sterling Connect:Direct log information and press **Enter**. The following is displayed:

```
You have chosen /logdirectory as the Sterling Connect:Direct log directory, please
confirm: [Y/n]
```

3. Press **Enter**. The following is displayed:

```
Enter the FULL path name of the Sterling Connect:Enterprise base log
directory: [/data/ceu2500/log]
```

4. Type a log directory or accept the default, and press **Enter**. The following is displayed:

```
You have chosen /logdirectory as the Sterling Connect:Enterprise log directory,
please confirm: [Y/n]
```

5. The following is displayed:

```
The script file /data/ceu2500/etc/cereport has been created!

To execute the Sterling Connect:Enterprise reporting tool, run cereport
at the shell prompt.

Sterling Connect:Enterprise File Agent Version 2.5.00 executed.

Would you like to return to the Sterling Connect:Enterprise
installation menu? [Y|n]
```

6. Press **Enter** to return to the installation menu. To exit the installation menu, type **n** and press **Enter**.

---

# Upgrading Sterling Connect:Enterprise for UNIX

This document covers the information you need when upgrading to Sterling Connect:Enterprise for UNIX Version 2.5.00 from a previous version of Sterling Connect:Mailbox for UNIX or Sterling Connect:Enterprise for UNIX.

The version of Sterling Connect:Enterprise for UNIX that you are upgrading from determines the upgrading considerations and procedures that you use. Refer to the following table as a guide to upgrading considerations and procedures:

| Upgrading From                                                  | Refer to                                                                                                                                                                              |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sterling Connect:Enterprise for UNIX version 2.4.04             | <ul style="list-style-type: none"><li>◆ <i>Upgrade Considerations for Version 2.4.04</i> on page 47</li><li>◆ <i>Running the Installation Script</i> on page 50</li></ul>             |
| Sterling Connect:Enterprise for UNIX version 2.4.03 and earlier | <ul style="list-style-type: none"><li>◆ <i>Upgrade Considerations for Version 2.4.03 and Earlier</i> on page 50</li><li>◆ <i>Running the Installation Script</i> on page 50</li></ul> |

---

## Upgrade Considerations for Version 2.4.04

Consider the following information when upgrading from Sterling Connect:Enterprise version 2.4.04:

If you use Password Encryption or Stored Batch Encryption, please read the following information and follow the instructions in *Upgrade and Fallback Planning* on page 49.

### New Encryption Ciphers for Password and Stored Batch Encryption

Sterling Connect:Enterprise for UNIX version 2.4.04 now supports the AES128 cipher for Password and Stored Batch encryption. However, it will no longer encrypt passwords or batches with the RC5 cipher, which was used on non-Linux platforms on previous releases. Sterling

Connect:Enterprise for UNIX version 2.5.00 will decrypt passwords and batches encrypted with RC5 from a previous release but will no longer encrypt with this cipher.

## Global Key Changes

Prior to Sterling Connect:Enterprise for UNIX version 2.4.04, the global key (\$CMUHOME/keys/key.global) and triple DES global key (deskey.global) were encrypted using Strong encryption (RC5 on non-Linux, RC4 on Linux). In Sterling Connect:Enterprise for UNIX version 2.4.04 and above, they are encrypted with RC4 in all cases. During the upgrade process, the ceukey -R utility is run to save the old keys into time stamped files and then reencrypt them with RC4. The ceukey -R utility tests the global key first and does nothing if it is already encrypted with RC4.

---

**Note:** The keys in RC4 format are not backward compatible with previous versions of Sterling Connect:Enterprise for UNIX on non-Linux platforms, so you must keep the time stamped saved copies for fallback purposes.

---

## Password Encryption Changes

Prior to Sterling Connect:Enterprise for UNIX version 2.4.00, encrypted passwords were stored in the RSD file using Strong encryption (RC5 on non-Linux, RC4 on Linux) based on the global key. The format was the following:

```
PASSWORD="ENCRYPTED_39E7FB8389CB1AB5" or
RMT_PASSWORD="ENCRYPTED_EC1BB4FA13F5498C"
```

Sterling Connect:Enterprise for UNIX version 2.5.00 will continue to read the old format and decrypt the passwords correctly but will no longer save passwords in this format.

In Sterling Connect:Enterprise for UNIX version 2.5.00, the Sterling Connect:Enterprise for UNIX administrator can specify the encryption to be used for password encryption in a new file \$CMUHOME/mcd/passencrypt.cfg. If the file is missing, the default cipher is RC4:

```
PASSWORD_ENCRYPT_CIPHER={DES|RC4|AES128|3DES}
```

As new RSDs are defined or users change their passwords, the PASSWORD field uses a new format to keep track of which cipher was used as shown in the following:

```
PASSWORD="ENCR_DES_XXXX..." (Password encrypted with DES)
PASSWORD="ENCR_RC_4_XXXX..." (Password encrypted with RC4)
PASSWORD="ENCR_AES1_XXXX..." (Password encrypted with AES128)
PASSWORD="ENCR_3DES_XXXX..." (Password encrypted with Triple DES)
```

---

**Note:** The passwords in the new format are not backward compatible with previous versions of Sterling Connect:Enterprise, so you should create a backup of your RSD directory for fallback purposes before you upgrade.

---



## Stored Batch Encryption Changes

Prior to Sterling Connect:Enterprise for UNIX version 2.4.04, batches could be encrypted with WEAK, STRONG, or 3DES encryption, based on settings in the \$CMUHOME/med/encrypt.cfg file. For WEAK and STRONG batches, the batch encryption key (unique for each batch) was itself encrypted with the global key using STRONG encryption (RC5 for non-Linux, RC4 for Linux) and stored in the batch header along with the encryption type (a one byte flag: “W” or “S”).

For triple-DES batches, the batch encryption key was (and still is) encrypted using triple-DES with the global triple-DES key and saved in the header with the encryption type (“T”). Triple-DES encryption is forward and backward compatible with Sterling Connect:Enterprise for UNIX version 2.5.00 and prior releases. The best strategy during an upgrade is to set triple-DES for all batches in the encrypt.cfg file as follows:

```
* Triple_DES      # Encrypts all new batches with 3DES encryption
```

Sterling Connect:Enterprise for UNIX version 2.5.00 reads batches encrypted in prior releases with WEAK or STRONG, but no longer encrypts batches in those formats. Instead, the batch encryption key is encrypted with the global key using RC4 and the actual batch encryption type is stored in the header (“D” for DES, “R” for RC4, “T” for Triple-DES, and “1” for AES128). If the encrypt.cfg file lists any batches to encrypt with WEAK or STRONG, the Sterling Connect:Enterprise for UNIX version 2.5.00 mailbox daemon will put out an error message and shut down. You must remove or comment out any references to WEAK or STRONG encryption in your encrypt.cfg file before you upgrade to CEU2500.

## Upgrade and Fallback Planning

When upgrading to Sterling Connect:Enterprise for UNIX version 2.5.00 complete the following steps to ensure a smooth upgrade and provide for a fallback to your previous release if needed.

1. Back up your \$CMUHOME/keys and \$CMUHOME/rsd directories prior to the upgrade. Restore them if you must fall back.
2. If you use Stored Batch Encryption, update your \$CMUHOME/med/encrypt.cfg prior to the upgrade to remove all references to WEAK or STRONG encryption and use Triple Des for encrypting all batches as follows:

```
* Triple_DES      # Encrypts all new batches with 3DES encryption
```

Any batches created after upgrading to Sterling Connect:Enterprise for UNIX version 2.5.00 will be readable by the pre-version 2.5.00 system.

---

## Upgrade Considerations for Version 2.4.03 and Earlier

Consider the following information when upgrading from Sterling Connect:Enterprise for UNIX version 2.4.03 and earlier:

### Encryption of Inbound AS2 Batches

If you had batch encryption enabled on the receiving mailbox on Sterling Connect:Enterprise for UNIX version 2.3.00, inbound batches may not be encrypted in Sterling Connect:Enterprise for UNIX version 2.5.00. If a dead letter mailbox is configured for the port receiving inbound AS2 batches, the dead letter mailbox is used to store inbound unprocessed AS2 batches as TR (transcript) or STG (staged) batches in Sterling Connect:Enterprise for UNIX version 2.5 which are then moved to the target mailbox after processing if this option is selected. If encryption is not enabled for the dead letter mailbox, the unprocessed AS2 batch will not be encrypted.

### Correlation of AS2 Batches

In Sterling Connect:Enterprise for UNIX version 2.5, .RQ, .NM, .MD, .OK, and .AS2 batch names include the batch number of the AS2 payload batch, which helps to correlate batches as they are processed.

The following cmulist output example shows batch correlation for an outbound batch:

|          |    |                    |      |                |       |        |
|----------|----|--------------------|------|----------------|-------|--------|
| sles8ssl | 15 | test_five.PL       | 5    | 06/01/23-17:11 | ARTZ  | psmil1 |
| sles8ssl | 16 | test_five.PL.15.RQ | 2395 | 06/01/23-17:11 | CRTWY | EDIINT |
| sles8ssl | 17 | test_five.PL.15.MD | 2967 | 06/01/23-17:11 | CGHY  | EDIINT |

The following cmulist output example shows batch correlation for an inbound batch:

|         |   |                          |     |                |      |        |
|---------|---|--------------------------|-----|----------------|------|--------|
| inbound | 4 | from-cerhas21-data.4.OK  | 5   | 06/01/23-15    | CWY  | EDIINT |
| inbound | 5 | from-cerhas21-data.4.AS2 | 401 | 06/01/23-15:   | CRWY | EDIINT |
| inbound | 6 | from-cerhas21-data.4.MD  | 864 | 06/01/23-15:56 | CWY  | EDIINT |

If you have backend automation setup on Sterling Connect:Enterprise for UNIX version 2.3.00 that is based on batch name, you will have to adjust your automation setup based on this new naming convention in Sterling Connect:Enterprise for UNIX version 2.5.00.

---

## Running the Installation Script

Use the following procedure to upgrade from Sterling Connect:Enterprise for UNIX version 2.3 or later. This procedure describes how to access the Sterling Connect:Enterprise for UNIX installation script, select the installation option, and specify the destination directory. You cannot install Sterling Connect:Enterprise for UNIX to networked storage media such as NFS or Samba shares.

1. Use one of the following methods for accessing the installation script:

- ◆ If you acquired your Sterling Connect:Enterprise installation from an ESD portal, navigate to the location of the **ceinstall** script.
  - ◆ If you acquired your Sterling Connect:Enterprise installation on a CD-ROM, mount the Sterling Connect:Enterprise for UNIX CD-ROM.
2. At the UNIX prompt, type:

```
ceinstall
```

3. Press **Enter**. The following introductory information is displayed:

```
IBM(R) Sterling Connect:Enterprise(R) for UNIX 2.5.00
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines

Installation Procedure

Please follow the Installation and Administration Guide and/or
Release Notes for the Sterling Connect:Enterprise component(s) to be installed.

UNIX(TM) is a registered trademark of The Open Group
=====
Press ENTER when ready.
```

4. Press **Enter**. The following prompt is displayed:

```
Enter the installation media location (mounted CD root, e.g. /cdrom/cdrom0/).
[/svshare/ceunix/2.5.00]:
```

5. Type the full path to the installation CD-ROM or Press **Enter** to accept the default. The installation menu is displayed.

```
Please select one of the following installation options:

(1) Install all Sterling Connect:Enterprise components
(2) Install or upgrade Sterling Connect:Enterprise base
(3) Install or upgrade Sterling Connect:Enterprise remote daemons
(4) Configure the Sterling Connect:Enterprise agents and cereport
(5) EXIT

Enter your choice:[1]
```

6. Type **2** and press **Enter**. A prompt similar to the following is displayed:

```
Sterling Connect:Enterprise base Version 2.5.00 will be installed in your system.
Do you want to continue? [Y|n]
```

7. Press **Enter**. A prompt similar to the following is displayed:

```
Enter the FULL path of the destination directory
into which to install Sterling Connect:Enterprise for UNIX Version 2.5.00.
You can use $HOME/ceunix to shorten the name:
[/install_directory]
```

---

**Note:** Do not use a dash (-) in the path of the destination directory.

---

8. Press **Enter**. A prompt similar to the following is displayed:

```
A previous installation of Sterling Connect:Enterprise has been detected in
/install_directory.
Would you like to upgrade the detected version? [Y|n]
```

9. Press **Enter**. A prompt similar to the following is displayed:

```
=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines
version 2.5.00 Upgrade Installation Procedure

You are beginning the Sterling Connect:Enterprise Upgrade Installation Procedure.
You have specified the following directory (called the destination directory)
/data/ahmi_ce2402
where the Sterling Connect:Enterprise files will be stored.

After the files are extracted from the media, a customization procedure will
be called. It will configure the Sterling Connect:Enterprise operating
environment for you.

UNIX(TM) is a trademark of X/Open Company, Ltd. in the U.S.A and other
countries.
=====

Press ENTER to continue.
```

10. Press **Enter**. A prompt similar to the following is displayed:

```
You have chosen /install_directory
as the destination directory. Please confirm: [Y|n]
```

11. Press **Enter**. A prompt similar to the following is displayed:

```
Existing files that are replaced by this update will be
backed-up to <filename>.replaced_by_patch2500.
```

```
New files added by this update that you may wish to
merge with your current installation will be added as
<filename>.new_in_patch2500. A summary of these
will be written to /install_directory/merge.2500.
```

```
Do you wish to continue? [Y|n]
```

12. Press **Enter**. A prompt similar to the following is displayed:

```
Approximately 250000 kbytes of disk space is required
to upgrade to Sterling Connect:Enterprise.
(Some of this space is needed for temporary files, and for saving existing files)
```

```
=====
Here is the current free disk space for each disk partition:
=====
```

| Filesystem   | 1024-blocks | Free     | %Used | Iused | %Iused | Mounted on   |
|--------------|-------------|----------|-------|-------|--------|--------------|
| /dev/hd4     | 6225920     | 4835324  | 23%   | 12038 | 1%     | /            |
| /dev/hd2     | 3014656     | 197876   | 94%   | 51192 | 7%     | /usr         |
| /dev/hd9var  | 1114112     | 837580   | 25%   | 4791  | 2%     | /var         |
| /dev/hd3     | 786432      | 490488   | 38%   | 993   | 1%     | /tmp         |
| /dev/hd1     | 1343488     | 1276720  | 5%    | 158   | 1%     | /export/home |
| /proc        | -           | -        | -     | -     | -      | /proc        |
| /dev/hd10opt | 196608      | 140368   | 29%   | 629   | 2%     | /opt         |
| /dev/data1v  | 98304000    | 83375704 | 16%   | 53267 | 1%     | /data        |

```
You have 83375704 kbytes of disk space available to you,
which is more than the required 250000 kbytes.
```

```
Do you wish to continue? [Y|n]
```

13. Type **Y** and press **Enter**. After the files are extracted and verified, the following prompt is displayed:

```
Sterling Connect:Enterprise files have been successfully upgraded and verified.
```

```
Press ENTER to continue the upgrade process.
```

14. The following is displayed:

```
.... removing commons-logging-api.jar
.... removing commons-logging.jar
.... removing EccpressoAll.jar
.... removing batik.jar
.... removing fop.jar
.... removing jcert.jar
.... removing jnet.jar
.... removing jakarta-regexp-1.2.jar
.... removing jaxb-api.jar
.... removing jaxb-libs.jar
.... removing jaxb-ri.jar
.... removing jaxp-api.jar
.... removing xalan.jar
Removing old jsp classes in /data/ahmi_ce2402/webservices/webapps/jsp
Creating /data/ahmi_ce2402/webservices/webapps/jsp/jsp dir
Web Admin directory is being renamed to:
/data/ahmi_ce2402/webservices/webapps/ceadmin.old
WebDAV directory is being renamed to:
/data/ahmi_ce2402/webservices/webapps/ceudav.old
Executing ceupgrade_release_2 Install Script.

The following existing files will be backed up and then replaced:
- profile, kshrc and cshrc;
- ceustartup and ceustartup.trace.
(This is in addition to what has already been backed up.)

Any modifications that you have made to these files will have to be
re-applied before starting the system.

Press ENTER to continue.
```

Press **Enter** to continue.

15. The following is displayed:

```

Making a copy of ./etc/profile
Making a copy of ./etc/kshrc
Making a copy of ./etc/cshrc
Making a copy of ./etc/ceustartup
Making a copy of ./etc/ceustartup.trace

...Creating /data/ahmi_ce2402/mcd/control.mcd.new.parameters....
Review this file for the new MCD parameters.

...Creating sample shell profiles (kshrc, cshrc and profile) in
/data/ahmi_ce2402/etc/ ....

...Creating C shell 'cshrc' file....

...Creating Korn shell 'kshrc' file....

...Creating Bourne shell 'profile' file....

Creating / Updating Roles Database ...

Role ISAM file exists. Performing upgrade. File index 1

Role ISAM file exists. Performing upgrade. File index 5

Role ISAM file exists. Performing upgrade. File index 15

Role ISAM file exists. Performing upgrade. File index 20

Roles database: Complete.

```

16. You are prompted with the following:

```

Do you want this userid [userID] to run the product and administer the Web Admin
Tool? [Y|n]

```

where *userID* is the user ID that is performing the installation. If you select *n* and press **Enter**, the *userID* that is installing the product cannot perform vital functions to Sterling Connect:Enterprise.

If you type *y* and press **Enter**, the following is displayed:

```

Giving administrative privileges to RSD

The administrator roles and accounts were created successfully.

```

## Customizing Sterling Connect:Enterprise for UNIX

The customization part of the installation depends on your current configuration. You will only be prompted to customize functionality that you are not currently using. For more information on customizing Sterling Connect:Enterprise for UNIX, see the following:

- ◆ *Setting Up Secure FTP* on page 30
- ◆ *Setting Up SSH* on page 32
- ◆ *Configuring High Availability* on page 34

- ◆ *Setting Up AS2* on page 35
- ◆ *Setting Up the HTTP Server* on page 36

For functionality that you are currently using, the installation script detects your existing configuration. For example, if you are using secure FTP in your current installation, the installation script detects your settings and you will not be prompted to set up secure FTP. Press **Enter** to continue with customization.

---

## Completing the Installation

After customization is complete, the installation script continues with the following:

```

Sterling Connect:Enterprise configuration completed.

        ----- NOTE -----
Before using Sterling Connect:Enterprise, please export the following
Sterling Connect:Enterprise environment variables.
export CMUHOME=/data/ahmi_ce2402
export CMUHOST=hostname
export CMUPOST=47267
export PATH=$PATH:$CMUHOME/etc:$CMUHOME/aix/bin:$CMUHOME/javali
export LD_LIBRARY_PATH=$CMUHOME/aix/lib
export LIBPATH=$CMUHOME/aix/lib
export SHLIB_PATH=$CMUHOME/aix/lib

You can set the environment variables by executing
. /data/ahmi_ce2402/etc/profile
at the shell prompt

        OR

incorporate [ $CMUHOME/etc/profile ]
into your environment.

=====

The new environment variables for shared objects must be defined to
the operating system before starting Sterling Connect:Enterprise.
See $CMUHOME/etc/profile, kshrc or cshrc for values.

IBM(R) Sterling Connect:Enterprise(R) for UNIX base Version 2.5.00 upgrade
successful.

Would you like to return to the Sterling Connect:Enterprise
installation menu? [Y|n]

```

If the upgrade script fails, refer to the upgrade log file, **ceupgradebase.userID.log**, located in the **/tmp** directory for information.

To return to the Sterling Connect:Enterprise for UNIX installation menu, press **Enter**. If you completed the installation, type **n** and press **Enter**. A command prompt is displayed.

After the upgrade completes successfully, refer to the *Chapter 4, Post-Installation Tasks*.



---

# Post-Installation Tasks

This chapter details the post-installation procedures for Sterling Connect:Enterprise. Post-installation comprises the following tasks:

- ◆ Exporting the environment variables
- ◆ Testing the system or manual customization
- ◆ Configuring the site administration user interface for third-party web server
- ◆ Setting the timeout values

You must perform the post-installation tasks before you can start Sterling Connect:Enterprise.

---

## Exporting the Environment Variables

During the Sterling Connect:Enterprise installation, you are given information on exporting the environment variables.

```

Sterling Connect:Enterprise configuration completed.

----- NOTE -----
Before using Sterling Connect:Enterprise, please export the following
Sterling Connect:Enterprise environment variables.

export CMUHOME=/data/ceu2500_base
export CMUHOST=hostname
export CMUPORT=8000
export PATH=$PATH:$CMUHOME/etc:$CMUHOME/aix/bin:$CMUHOME/javali
export LD_LIBRARY_PATH=$CMUHOME/aix/lib
export LIBPATH=$CMUHOME/aix/lib
export SHLIB_PATH=$CMUHOME/aix/lib

You can set the environment variables by executing
. /data/ceu2500_base/etc/profile
at the shell prompt

OR

incorporate $CMUHOME/etc/profile
into your environment.

=====

Please press ENTER to continue...

```

The environment variables are exported after the Sterling Connect:Enterprise installation script has been executed.

---

**Note:** If you upgraded from a previous version of Sterling Connect:Enterprise for UNIX or Sterling Connect:Mailbox for UNIX, you do not need to export the environment variables.

---

Set your environment variables by using the appropriate shell commands for the Bourne, C, or Korn shells to create the environment variables in the *\$CMUHOME/etc/profile*, *cshrc*, or *kshrc* files. Add these variables to your own *.profile*, *.cshrc*, or *.kshrc* files as needed using an editor such as *vi* to add the variables.

For example, the following command is appropriate if you are adding the *CMUHOME* variable to your *.cshrc* shell.

```
setenv CMUHOME $HOME/ceunix
```

The following command is appropriate if you are adding the *CMUHOME* variable to your *.kshrc* shell.

```
CMUHOME=$HOME/ceunix; export CMUHOME
```

The following table describes the environment variables used with Sterling Connect:Enterprise.

| Variable                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CMUHOME                        | Home or destination directory, containing all the Sterling Connect:Enterprise files, for example, <i>/usr/home/ceunix</i> .                                                                                                                                                                                                                                                                                                                                   |
| CMUHOST                        | UNIX host name where the Sterling Connect:Enterprise Control daemon ( <i>cmuctld</i> ) is running.                                                                                                                                                                                                                                                                                                                                                            |
| CMUPOINT                       | TCP/IP port number of <i>cmuctld</i> .                                                                                                                                                                                                                                                                                                                                                                                                                        |
| CMUPASWD                       | Password required for your user ID to Sterling Connect:Enterprise. If you do not specify this environment variable, then you are prompted for a password each time you invoke a Sterling Connect:Enterprise command.<br><br>Note: Setting this environment variable compromises the security of Sterling Connect:Enterprise. To take advantage of the security features built into Sterling Connect:Enterprise, do not set the CMUPASWD environment variable. |
| RTICDIR<br>(ARTIC Bisync only) | This variable must be set to point to the directory where the Bisync Runtime library is installed. An example is <i>/usr/lpp/dcplib</i> . For bisync functionality, set RTICDIR and PATH to include the path where ARTIC drivers and utilities are installed, specifically the files <i>icaaim.com</i> and <i>icarc.com</i> , which come in the <i>\$CMUHOME/etc</i> directory, and <i>icaldric</i> , which you must obtain yourself.                         |
| PATH                           | The PATH variable needs to include the correct path to the Sterling Connect:Enterprise <i>/bin</i> and <i>/etc</i> subdirectories. If you are running on an AIX system, then add <i>\$CMUHOME/aix/bin</i> to the PATH variable. For HP systems, add <i>\$CMUHOME/hpux/bin</i> . For Solaris systems, add <i>\$CMUNIX/sun/bin</i> . For Linux Systems add <i>\$CMUHOME/linux/bin</i> .                                                                         |
| MANPATH                        | The MANPATH variable sets the search path used by the <i>man</i> command to locate Sterling Connect:Enterprise man pages. The search path is a list of directories separated by a colon (:) in which the manual subdirectories can be found. For example, <i>MANPATH=\$MANPATH:\$CMUHOME/man</i> .                                                                                                                                                            |

## Testing the Installation

Prior to starting Sterling Connect:Enterprise, the installation may be tested using **cmu\_quick\_test**. After running **cmu\_quick\_test**, continue with the *Setting Up the Sterling Connect:Enterprise for UNIX Site Administration User Interface* on page 65.

The following steps give instructions on running the test script:

1. Type the following command:

```
cmu_quick_test
```

The test script starts.

```
=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX (C) Copyright IBM Corp. 1994, 2011
All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines

version n.n.nn Installation Test

This test should be run only after product installation is complete!
=====

Press ENTER when ready or Ctrl-C to exit.
```

2. Press **Enter** to begin the test or **Ctrl+C** to exit. The following prompt is displayed.

```
Enter full path of Sterling Connect:Enterprise home directory:
[/usr/mailbox/ceunix]:
```

3. Press **Enter** to accept the default location.

```
Now running the installation test.....

Starting IBM(R) Sterling Connect:Enterprise(R) for UNIX system...
```

---

**Note:** The system pauses for approximately five seconds while Sterling Connect:Enterprise starts. Your screen then shows the progress made in the initialization of the various Sterling Connect:Enterprise processes.

---

```

cmuctld...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Secure Mailbox Control Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX 2.5.00 Build 44 CEUCVTREP utility
  cmuauthd...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Authentication Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
  cmumboxd...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Secure Mailbox Engine Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
      Mailbox daemon - Active records in database: 4
      Mailbox daemon - Highest batch number       : 4
  cmusvid...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Service Interface Daemon
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
  cmuacd...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Auto connect Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
  cmuexitd...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Exits Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
  cmulogd...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Log Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
  cmuftp...

```

```

IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
FTP Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX FTP Server [FTP,SSL=NONE] active on
0.0.0.0:47386
  cmusshftpd...
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
SSH FTP Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX SSH Server [SSHFTP] active on
0.0.0.0:47390
-----
      All of the core daemons have been started.
Please verify that no errors were reported before
continuing with the command line utilities.
-----

Please press ENTER to run cmusession...

```

4. Press **Enter** to run the **cmusession** utility. This utility shows the status of the communication resources.

```

Date: 03/02/11          IBM Sterling Connect:Enterprise for UNIX+
Page: 0001
Time: 20:26:30          Session Utility

Command Line Parameters:
  cmusession

Name      Type      Host      PID      RmtID      Resource
State          SID

SSHFTP    Master      gasol10   1859     47390
Idle      10
FTP       Master      gasol10   1856     47386
Idle      9
ACD       Master      gasol10   1848
-         4

Max. Concurrent Sessions: 0

```

5. Press **Enter** to run the **cmuadd** utility. This utility adds a test file to the repository.

```

Date: 03/02/11          IBM Sterling Connect:Enterp+          Page: 0001
Time: 20:32:12          ADD Utility

Command Line Parameters:
  cmuadd
  -iqatest
  -btest batch
  -m

Mbx ID   Batch #   Batch ID   Bytes   Date-Time   Status   Org ID
-----
qatest   4          test batch 100     11/03/02-20:32  ARMZ    qatest

Input Files Processed
File Name      File Size      Pr Status

Summary Information
Number of Batches Added:    1
Date: 03/02/11          IBM Sterling Connect:Enterp+          Page: 0002
Time: 20:32:12          ADD Utility

Number of Input Files:      0
Number of Files Bypassed:   0
Number of Input Bytes:     100

```

---

**Note:** The test file, test.data, is a small ASCII file that is included in the distribution.

---

6. Press **Enter** to run the **cmulist** utility. This utility lists the contents of the repository and provides the Batch Status Code values.
7. Verify that the test file you just added is listed.

```

Date: 03/02/11          IBM Sterling Connect:Enterprise for UNIX+
Page: 0001
Time: 20:33:52          LIST Utility

Command Line Parameters:
    cmulist

Batch Status Code Values:
A - Added Offline           D - Flagged for Delete
I - Incomplete Collection   C - Collected online
T - Online Transmit Done    R - Online Request Allowed
E - Extracted batch         M - Multiple transmission
P - Transmission in Progress U - Batch Unextractable
N - Batch Nontransmittable  B - BSC
F - FTP                     W - AS2
K - EBCDIC                  H - HTTP
Y - BINARY                  Q - ASYNC
G - SSL                     S - LOG batch
X - Transparent Bisync Index=Yes O - Batch Encryption
Z - ASCII                   V - BP Verified
L - SSHFTP                  J - Business Process

Mbx ID      Batch #      Batch I'D      Bytes      Date-Time      Status      Org ID

gatest      4              test batch     100        11/03/02-20:32 ARMZ      gatest
user1       1              file1          757        11/03/02-20:11 ARMZ      gatest
Date: 03/02/11          IBM Sterling Connect:Enterprise for UNIX+
Page: 0002
Time: 20:33:52          LIST Utility

user1       2              file1          757        11/03/02-20:17 ARMZ      gatest
user1       3              file1          30750000  11/03/02-20:20 ARMZ      gatest

Please press ENTER to continue ....

Please enter the Sterling Connect:Enterprise admin password:
The Message Agent is not active.
Shutdown quiesce requested.
Active sessions may delay shutdown.
System Down.
Please press ENTER to continue ....

```

8. Press **Enter** to continue.

```
End of IBM(R) Sterling Connect:Enterprise(R) for UNIX Installation Test.
```



---

## Remove userid.log Files

You must remove the `/tmp/ceinstall.userid.log` and `/tmp/directinstall.userid.log` files after validating the installation, where *userid* is the user ID that performed the installation.

---

## Setting Up the Sterling Connect:Enterprise for UNIX Site Administration User Interface

Sterling Connect:Enterprise installs a Web server configured for use with the Site Administration user interface. However, if you want to run the Site Administration interface on a third-party Web server, you must complete the following procedures.

### Configuring the Site Administration User Interface for Third-Party Web Server

Before you start the procedure, complete the following tasks:

- ◆ Install and configure your Web server and servlet engine.
  - ◆ Verify that there are communications between them.
1. Using your Web server, deploy the `ceadmin.war` file located in the `$CMUHOME/webservices` directory, but do not start your Web server.

---

**Note:** Depending on the Web server, you may need to start the Web server to deploy it for the first time. Then you can edit the system properties and restart the server.

---

2. Navigate to the following directory:

`Deploy_Directory/ceadmin/property`

where *Deploy\_Directory* is the directory where the `ceadmin.war` file is deployed.

---

**Note:** This directory may also be `Deploy_Directory/ceadmin.war/property`

---

3. Verify that the `system.properties` file identifies the correct host name and port where the Sterling Connect:Enterprise for UNIX service daemon is running. This information was required in *step 8 on page 23 of Before You Begin* on page 21. The default the installation script provides is 8001.
4. Start or restart your Web server.
5. Use the following URL to run the Sterling Connect:Enterprise for UNIX Site Administration User Interface:

`http://servername:port/ceadmin/jsp/index.jsp`

6. Log on to the Sterling Connect:Enterprise for UNIX Site Administration user interface with user ID and password defined during installation. Both of these user IDs have Administrator access. For security reasons, change the passwords for these user IDs after you log on.

## Setting the Timeout Values

When setting up the Site Administration user interface, consider the following information.

The timeout values determine how frequently the browser must interact with the Sterling Connect:Enterprise for UNIX server before the session is closed. If you exceed the lowest of these timeout values while making updates, your changes are lost and you are logged off the system. The timeout for the Site Administration user interface is defined in two places:

- ◆ In the Service Interface daemon, **cmusvid**, the default session value determines how long the Sterling Connect:Enterprise for UNIX server waits for information from the Web server. The initial value is 10 minutes (600 seconds). Change the value of the **-T** parameter to increase the session timeout. In the following example, the session timeout is increased to 1900 seconds:

```
cmusvid -H hostname -P 7607 -p 7606 -d cmusvid.out -l 9 -T 1900 &
```

Refer to the *cmusvid—Service Interface Daemon* on page 82 for more information.

- ◆ Browsers have a default timeout value of 30 minutes. You can change this default timeout using the following procedure:
  - a. Navigate to the following directory:

```
Deploy_Directory/ceadmin/WEB-INF
```

where *Deploy\_Directory* is the directory where the *ceadmin.war* file is deployed.

---

**Note:** This directory may also be *Deploy\_Directory/ceadmin.war/WEB-INF*

---

- b. Open the *web.xml* file.
- c. Find the following XML tag:

```
<param-name>timeout</param-name>
<param-value>30</param-value>
```

If you set this parameter above 30, it will override the default browser timeout of 30 minutes. If you set this value at or below 30, the default browser timeout of 30 minutes is used.

---

## Configuring Role-Based Access

After you configure the Sterling Connect:Enterprise for UNIX Site Administration user interface, you must design and implement a role-based access system to enable users to perform tasks from the interface. See Chapter 6, *Role-Based Access*, for detailed information and procedures to assist you in developing a role-based access system.



---

# Starting and Stopping Sterling Connect:Enterprise

After completing the installation and configuration of Sterling Connect:Enterprise, you are ready to start using the system. This chapter describes how to start and stop Sterling Connect:Enterprise.

---

## Startup Script

Sterling Connect:Enterprise is usually started using a script, **ceustartup**, that is created during the installation procedure. The script starts each server (daemon) from the command line, using values provided during installation as reference points for parameter value assignments. Verify the settings in *\$CMUHOME/etc/ceustartup* and make any modifications before you start Sterling Connect:Enterprise for the first time. For information on how to modify the **ceustartup** script, see the *Modifying Startup Scripts* on page 72.

### Starting Sterling Connect:Enterprise with ceustartup

To start Sterling Connect:Enterprise, enter the **ceustartup** command at the prompt.

```
ceustartup
```

Sterling Connect:Enterprise lists each daemon and its status in the order it is started. Read the output of **ceustartup** carefully whenever changes are made to the script. The following output shows the recommended start order for the daemons.

```
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines
Starting Sterling Connect:Enterprise.
IBM Sterling Connect:Enterprise for UNIX 2.5.00 Build 44 CEUCVTREP utility
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Secure Mailbox Control Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX 2.5.00 Build 44 CEUCVTREP utility
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Authentication Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Secure Mailbox Engine Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
    Mailbox daemon - Active records in database: 4
    Mailbox daemon - Highest batch number      : 4
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Auto connect Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Log Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Exits Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
Service Interface Daemon
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
20:40:22: Starting Sterling Connect:Enterprise ADMIN/WebDAV Daemon as Resource
"ADMIN"
```

```

IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
FTP Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX FTP Server [FTP,SSL=NONE] active on
0.0.0.0:47386

IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
FTP Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX FTP Server [FTP_AUTO,SSL=NONE] active on
0.0.0.0:47388
IBM Sterling Connect:Enterprise for UNIX V2.5.00 Build 44
SSH FTP Server
Copyright 1994, 2011 All Rights Reserved
Connect:Enterprise is a trademark of IBM Corp.
All rights reserved.
U.S. Patent Numbers 5,734,820 6,981,278
IBM Sterling Connect:Enterprise for UNIX SSH Server [SSHFTP] active on 0.0.0.0:47390
20:40:30: Starting Sterling Connect:Enterprise HTTP Daemon as Resource "HTTP"
20:40:35: Starting Sterling Connect:Enterprise EDIINT Daemon as Resource "EDIINT"
To start the web interface, open your browser to:
  http://servername:port/ceuadmin/jsp/index.jsp
Starting the File Agent

```

---

Note: If you used a passphrase for the SSH host key (during installation), run the following command after startup: `cmurefresh -s <passphrase>`, where `<passphrase>` is the `ssh_host_key` passphrase.

---

## Starting Sterling Connect:Enterprise in Debug Mode

In addition to the `ceustartup` script, the installation process also generates the `ceustartup.trace` script. This script can be used in place of `ceustartup` when you need to diagnose problems with Sterling Connect:Enterprise.

---

**Caution:** Start Sterling Connect:Enterprise for UNIX with `ceustartup.trace` only when instructed by IBM Customer Services personnel because this action degrades performance.

---

You can also trace Sterling Connect:Enterprise resources using the dynamic tracing feature. Refer to *Tracing Sterling Connect:Enterprise Activity* on page 139.

`ceustartup.trace` script is identical to the `ceustartup` script except that all the daemons are started with the `-l 9` (message level 9) parameter and the `-d` debug file path and file name to capture debug messages from each of the daemons. This script can be modified to specify a message debug level

between 0 and 99, with 99 defined as extremely verbose. For **cmuediintd** and **cmuhttpd**, valid debug levels are 0-98.

Any changes made to the **ceustartup** script should be duplicated in the **ceustartup.trace** script to customize the script for your system configuration. For information on how to modify the **ceustartup.trace** script, see the *Modifying Startup Scripts* on page 72.

Use the following steps to run **ceustartup.trace**:

1. Before starting Sterling Connect:Enterprise for the first time with debug messages, verify the settings in the **ceustartup.trace** script and make any necessary modifications.
2. Type the **ceustartup.trace** command at the prompt.

```
ceustartup.trace
```

---

Note: If you used a passphrase for the SSH host key (during installation), run the following command after startup: `cmurefresh -s <passphrase>`, where `<passphrase>` is the `ssh_host_key` passphrase.

---

## Modifying Startup Scripts

Both **ceustartup** and **ceustartup.trace** can be modified to meet your unique Sterling Connect:Enterprise needs. You can use a text editor, such as `vi`, to modify the files, which are located in the `$CMUHOME/etc` directory.

The main function of the startup scripts is to start all the daemons with the appropriate switches and in the correct sequence. The following daemons are started from the command line: **cmuctld**, **cmuauthd**, **cmumboxd**, **cmulogd**, **cmuacd**, **cmuexitd**, **cmusvid**, **cmuadmind**, **cmuasyd**, **cmuftpd**, **cmubscda**, **cmubscdc**, **cmuhttpd**, **cmuediintd**, **cmusshftpd**.

The following daemons are required: **cmuctld**, **cmuauthd**, **cmumboxd**, **cmulogd**, **cmuacd**, and **cmuexitd**.

Only one instance of each of the required daemons is started for a single installation of the product. All required daemons should run on the same host server.

---

Note: More than one installation of Sterling Connect:Enterprise can execute on a single host or network, but each set must be complete with a unique repository database, unique Control daemon and FTP daemon port numbers, definitions files, and Communications daemons with their attendant hardware resource.

---

In addition to the required daemons, a single installation of Sterling Connect:Enterprise must have at least one of the Communications daemons (AS2, Async, Bisync for ARTIC, Bisync for Cleo, FTP, or Secure FTP). The system also allows multiple Communications daemons for a single protocol. For example, one Sterling Connect:Enterprise can be served by a single FTP daemon with no Async or Bisync daemons. Another Sterling Connect:Enterprise can have three Async daemons and two Bisync daemons.



The daemon order in the startup scripts must be maintained for all user modifications. This sequence is

1. cmuctld
2. cmuauthd
3. cmumboxd
4. cmuacd
5. cmulogd
6. cmuexitd
7. cmusvid
8. cmuadmind
9. **cmuasyd** and/or **cmuftpd** and/or **cmubscda** and/or **cmubscdc** and/or **cmuhttpd** and/or **cmuediintd** and/or **cmusshftpd**

## Configuring FTP to Use SOCKS Protocol

To configure Sterling Connect:Enterprise to use the SOCKS protocol for FTP connectivity, you must add the following parameters to the ceustartup script. These parameters must occur in the ceustartup script before cmuftpd.

| Parameter    | Description                                                                                                                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SOCKS_SERVER | Fully qualified domain name or an IP address of the SOCKS proxy server on a network. If you use the fully qualified domain name, DNS resolution must be enabled on the Sterling Connect:Enterprise host computer. |
| SOCKS_NS     | Defines the IP address of the Name server. Do not specify this if normal DNS services is working properly. If specified, this must be an IP address, not a domain name.                                           |
| SOCKS_DNAME  | Defines the default domain used for requests to the Name server. Specify this if simple host names are being used for SOCKS connections to specify the default Name Server Domain.                                |

## cmuctld—Control Daemon

Started first, this daemon coordinates the starting of the other daemons by establishing a well-known port that the other daemons must log in to. This port number is specified through a command line parameter when the Control daemon is started. The port number and the host name or IP address of the Control daemon must be provided through command line parameters to all the other daemons as they are started. Sockets are established between the daemons to support command and data message traffic through the TCP/IP network.

## cmuctld Parameters

All **cmuctld** parameters are optional. The parameters for **cmuctld** are described in the following table.

| Parameter | Value                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -C        | MCD configuration file | Overrides the default MCD file name. The default is <i>\$CMUHOME/mcd/control.mcd</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -d        | debugfile              | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -H        | hostname               | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l        | debug level            | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -P        | portno                 | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -Q        | nnnn                   | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems. <b>CAUTION:</b> Use this switch only when instructed to do so by IBM Support or Development.                                                                                                                                                                                                                                                                                   |
| -r        | directory of RSD files | Specifies another directory location for the RSD files, rather than the default of <i>\$CMUHOME/rsd</i> .<br><b>Caution:</b> Specifying an alternate directory for the RSD files makes them inaccessible from the Site Administration user interface.                                                                                                                                                                                                                                                                                                                                                                                                     |
| -? -h     |                        | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## cmuauthd—Authentication Server Daemon

The authentication server daemon enforces the password policies when a user logs on to Sterling Connect:Enterprise for UNIX. It first checks the password administration configuration file and determines whether a password policy is enforced, then it determines how to enforce the policy using information in the RSD policy files.

| Command | Parameter      | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -D      | <i>seconds</i> | Specifies the delay in seconds between starting the external authentication server and attempting to connect to the external authentication server. Default is 5 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -d      | debugfile      | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| -H      | hostname       | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                                                                                                                                   |
| -l      | debug level    | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -P      | portno         | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> The Authentication Server daemon will use the port value on less than the port the Control Daemon is using. |

| Command | Parameter | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -p      | portno    | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail. |
| -Q      | nnnn      | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.                                                                                                                                                                        |
| -? -h   |           | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## cmumboxd—Mailbox Daemon

The Mailbox daemon parses *\$CMUHOME/med/cmumbox.med* and performs all read and write actions to the repository directories. This includes actual data batches as well as their control records. The Communications daemons (*cmuasyd*, *cmuftp*, *cmubscda*, and *cmubscdc*) pass data and command messages to and from the Mailbox daemon through a TCP/IP connection. The Mailbox daemon also serves the command line utilities used at the local site, such as **cmuadd** and **cmuextract**.

### cmumboxd Parameters

All **cmumboxd** parameters are optional. The parameters for **cmumboxd** are described in the following table:

| Parameter | Value                  | Description                                                                                                                                                                                                                            |
|-----------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -b        | nnnn                   | Specifies the byte count interval that is reported by system status updates. Default is 0 (disabled).                                                                                                                                  |
| -C        | MCD configuration file | Overrides the default MCD file name. The default is <i>\$CMUHOME/mcd/control.mcd</i> .                                                                                                                                                 |
| -d        | debugfile              | Specifies the debug message output file name.                                                                                                                                                                                          |
| -e        | none                   | Controls whether or not the Batch Receive Informer and Batch Receive Exit are called when a RENAME command is submitted. If this parameter is not in the startup script, Batch Receive Informer and Batch Receive Exit are not called. |

| Parameter | Value                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -H        | hostname             | <p>Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is:</p> <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l        | debug level          | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| -P        | portno               | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p        | portno               | <p>Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.</p>                                                                                                         |
| -Q        | nnnn                 | <p>Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.</p> <p><b>CAUTION:</b> Use this switch only when instructed to do so by IBM Support or Development.</p>                                                                                                                                                                                                                                                                            |
| -r        | <none>               | <p>Specifies that the <b>mbxacl.conf</b> file is used to enact restricted access for mailbox security. If <b>-r</b> is not specified, all users have full access to all mailboxes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| -s        | system administrator | <p>Only valid if <b>-r</b> is used. The <b>-s</b> allows the account that started the Mailbox daemon to designate another account as the system administrator. If <b>-s</b> is not specified with <b>-r</b> in effect, the system administrator is the account that started the Mailbox daemon.</p>                                                                                                                                                                                                                                                                                                                                                              |
| -? -h     |                      | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## cmulogd—Log Daemon

The Log daemon records log messages from the Auto Connect daemon, the Communications daemons, and command line utilities. How many are saved and the maximum size of these files are determined by the **Maximum number of log files** and **Maximum log file size (KB)** parameters in the **control.mcd** file. These values are set in Define Configuration function of the Site Administration user interface. The log messages are later formatted by the **cmureport** utility.

If **cmulogd** detects that it can no longer write to the log file because the disk is full, it prints an error message to the standard error (stderr) on your system. It also initiates the shutdown immediate procedure.

### cmulogd Parameters

All **cmulogd** parameters are optional. The parameters for **cmulogd** are listed in the following table:

| Parameter | Values        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d        | debugfile     | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -e        | exit on error | Specifies that if a logging error occurs, Sterling Connect:Enterprise for UNIX is shutdown.                                                                                                                                                                                                                                                                                                                                                                                         |
| -H        | hostname      | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul> |
| -l        | debug level   | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -n        |               | Instructs the log daemon to “normalize” the start and/or end timestamps on each incoming record to the current time on the log daemon machine. This ensures that all records written are based on one clock and will not have time discrepancies due to running protocol daemons on another machine. Without the -n flag, no alteration is done on the records.                                                                                                                     |

| Parameter | Values    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -P        | portno    | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMU <code>PORT</code> environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a <code>getservbyname()</code> call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p        | portno    | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to <code>stderr</code> and the daemon startup will fail.                                                                                                                       |
| -Q        | nnnn      | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.                                                                                                                                                                                                                                                                                                           |
| -S        | pipe name | Specifies the name and location of the <code>cmuuserlog</code> utility: <code>\$CMUHOME/arch.bin/cmuuserlog</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| -? -h     |           | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## cmuacd—Auto Connect Daemon

The Auto Connect daemon parses the ACD files at startup and when **cmurefresh** is executed. In addition to initiating fully automated auto connects as dictated by the `WHEN=` parameters within one or more ACD files, the Auto Connect daemon serves the **cmuconnect** command by invoking manual auto connects. This daemon also manages the queuing of failed auto connects and processes ACDs for automatic routing. Log messages issued to the Log daemon by **cmuacd** are later formatted by the **cmureport** utility to produce Auto Connect Detail and Summary reports as well as Queued Auto Connect queuing reports.

---

Note: When the system time changes, for example during daylight savings time, you must run the `cmurefresh` command to update auto connects (scheduled transfers) with the new system time.

---

## cmuacd Parameters

All **cmuacd** parameters are optional. The parameters for **cmuacd** are listed in the following table:

| Parameter | Values      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d        | debugfile   | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -H        | hostname    | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l        | debug level | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -N        | Daemon Name | Overrides the default daemon name of ACD. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| -P        | portno      | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p        | portno      | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.                                                                                                         |
| -Q        | nnnn        | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.                                                                                                                                                                                                                                                                                |



| Parameter | Values        | Description                                                                                                                                                                                                                            |
|-----------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r        | ACD directory | Overrides the default ACD directory path name. The default is <code>\$CMUHOME/acd</code> .<br><b>Caution:</b> Specifying an alternate directory for the RSD files makes them inaccessible from the Site Administration user interface. |
| -? -h     |               | Displays the usage message.                                                                                                                                                                                                            |

## cmuexitd—Exit Daemon

The Exit daemon makes calls to the exit functions when triggered by the appropriate events. For example, the batch receive exit is invoked upon receipt of the EOF indicator when the last record of a batch is collected online.

### cmuexitd Parameters

All **cmuexitd** parameters are optional. The parameters for **cmuexitd** are listed in the following table:

| Parameter | Value       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d        | debugfile   | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -H        | hostname    | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul> |
| -l        | debug level | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -N        | Daemon Name | Overrides the default daemon name. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                      |

| Parameter | Value  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -P        | portno | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMU <code>PORT</code> environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a <code>getservbyname()</code> call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p        | portno | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to <code>stderr</code> and the daemon startup will fail.                                                                                                                       |
| -Q        | nnnn   | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.                                                                                                                                                                                                                                                                                                           |
| -? -h     |        | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### cmusvid—Service Interface Daemon

The service interface daemon manages all communication between the Sterling Connect:Enterprise for UNIX Site Administration user interface and the Sterling Connect:Enterprise for UNIX server.

| Command | Parameter | Associated Values                             |
|---------|-----------|-----------------------------------------------|
| -d      | debugfile | Specifies the debug message output file name. |

| Command | Parameter   | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -H      | hostname    | <p>Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is:</p> <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                                                                                                                                   |
| -N      | Daemon Name | <p>Overrides the default daemon name. Daemon names should be 8 characters or less with no spaces.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -l      | debug level | <p>Specifies the debug message level.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -P      | portno      | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used. The Authentication Server daemon will use the port value on less than the port the Control Daemon is using.</li> </ul> |
| -p      | portno      | <p>Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.</p>                                                                                                                                                                                                                     |
| -Q      | nnnn        | <p>Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.</p> <p><b>CAUTION:</b> Use this switch only when instructed to do so by IBM Support or Development.</p>                                                                                                                                                                                                                                                                                                                                                                                        |

| Command | Parameter | Associated Values                                                                                                                                                                      |
|---------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -S      | sessions  | Specifies the maximum number of sessions with the Site Administrator user interface that are supported. The default value is 150.                                                      |
| -T      | timeout   | Specifies the session timeout value in seconds. The default value is 600. Sessions with the Site Administrator user interface time out when a period of inactivity exceeds this limit. |
| -? -h   |           | Displays the usage message.                                                                                                                                                            |

## cmuadmind—Administration Daemon

The administration daemon enables Sterling Connect:Enterprise for UNIX to provide an internal Java HTTP server and servlet for the Sterling Connect:Enterprise for UNIX Site Administration interface. With **cmuadmind**, you are not required to install a third-party Web server. The administration daemon also serves remote sites that use WebDAV commands.

The parameters for **cmuadmind** are listed in the following table:

| Command | Parameter   | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -w      | portno      | Specifies the port that the Java HTTP server (Jetty server) monitors for communication from Web browsers. These messages are then passed to the Service Interface Daemon (cmusvid). This parameter is not required. The port number was automatically provided in an .xml file during the installation of Sterling Connect:Enterprise for UNIX. Use this parameter only if you need to override the installed port number.                                          |
| -d      | debugfile   | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -H      | hostname    | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ Value passed on the command line using the <b>-H</b> parameter</li> <li>◆ Value of the CMUHOST environment variable</li> <li>◆ Value of the gethostname() system call</li> <li>◆ Literal value of <i>localhost</i></li> </ul> |
| -N      | Daemon Name | Overrides the default daemon name. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                      |
| -l      | debug level | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Command | Parameter    | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -P      | portno       | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMU<code>PORT</code> environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a <code>getservbyname()</code> call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> <p>The Authentication Server daemon will use the port value on less than the port the Control Daemon is using.</p> |
| -p      | portno       | <p>Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to <code>stderr</code> and the daemon startup fails.</p>                                                                                                                                                                                                                                             |
| -Q      | nnnn         | <p>Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.</p> <p><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| -x      | max sessions | <p>Specifies the maximum number of sessions with the Site Administration user interface that are supported. The default value is 20.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| -T      | timeout      | <p>Specifies the session timeout value in seconds. The default value is 600. Sessions with the Site Administration user interface time out when a period of inactivity exceeds this limit.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| -? -h   |              | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## cmuasysd—Async Daemon

The Async daemon serves remote sites using XMODEM, YMODEM, ZMODEM, Kermit, or ASCII protocols and asynchronous modems.

XMODEM support can be interactive or non-interactive. When remote connects occur, log messages are sent to the Log daemon that are later formatted by the **cmureport** utility to produce Remote Connect Detail and Summary reports. This daemon is not required if at least one other

Communications daemon is executing. More than one Async daemon can serve a single repository, but each must use unique CPD files and unique devices defined in the CPD files.

### cmuasyd Parameters

The parameters for **cmuasyd** are listed below.

| Parameter | Value                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -C        | CPD configuration file | Overrides the default CPD file name. The default is <i>\$CMUHOME/cpd/async.cpd</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| -d        | debugfile              | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -H        | hostname               | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l        | debug level            | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -N        | <i>daemon Name</i>     | Overrides the default daemon name of ASYNC. This parameter is required if multiple Async daemons are running. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| -P        | portno                 | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p        | portno                 | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.                                                                                                         |

| Parameter | Value | Description                                                                                                                                                                                                                                                                                                                                                                |
|-----------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -Q        | nnnn  | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development. |
| -? -h     |       | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                |

## cmuftp—FTP Daemon

There are four distinct FTP daemons: *cmuftp* (the master daemon) and the three slave daemons it forks for individual connections:

- ❖ *ftpd* (server slave used for remote connects)
- ❖ *ftp* (client slave used for auto connects)
- ❖ *rftp* (SOCKS-enabled client slave used for auto connects that must navigate SOCKS firewalls)

The FTP daemon serves remote sites using the FTP commands **get**, **put**, and **mput** through a port listener. The FTP remote sites are usually connected to a network without the use of modems at the FTP daemon's host. The FTP daemon itself provides no modem support. Dial-up FTP remotes connect to the network using SLIP or PPP connections established independently of Sterling Connect:Enterprise.

If you are using FTP scripting for security, you must specify the firewall information in the **Specify FTP Firewall** screen in the Site Administration user interface. There are four pieces of information that the FTP client needs to traverse a single firewall:

- ❖ IP address of the firewall host running the *ftpd* proxy server
- ❖ Port number at which the *ftpd* proxy server is listening
- ❖ Valid login ID of a user of the firewall host
- ❖ Valid password for the above login ID

The **Specify FTP Firewall** parameters allow the Sterling Connect:Enterprise FTP client to traverse intermediate FTP proxy servers. Secure FTP cannot be used with FTP proxy firewalls.

The FTP daemon in Sterling Connect:Enterprise also has the capability to cross the local SOCKS-based firewall (either inbound or outbound) by using a binary named **rftp**. By default, *cmuftp* does not use this binary. To use the binary to cross the SOCKS firewall, start *cmuftp* with parameter **-S**.

All clients that cross the local SOCKS firewall refer to the */etc/socks.conf* file to navigate the firewall. The *socks.conf* file contains the information, such as the IP address of the host running sockd server, destination IP address, and so forth.

After a remote site establishes a TCP/IP connection with the host where *cmuftp* is executing, an FTP login can be made with Sterling Connect:Enterprise to begin a remote connect session. When

remote connects occur, log messages are sent by *cmuftp* to the Log daemon that are later formatted by the *cmureport* utility to produce Remote Connect Detail and Summary reports. More than one FTP daemon can serve a single repository, but each must use unique CPD files and unique port listeners must be defined in each CPD. This is set up using the Site Administration user interface.

### cmuftp Parameters

All *cmuftp* parameters are optional. The parameters for *cmuftp* are described in the following table:

| Parameter | Value                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -C        | CPD configuration file | Overrides the default CPD file name. The default is <i>\$CMUHOME/cpd/ftp.cpd</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -c        | FTP client pathname    | Overrides the <b>FTP client path</b> parameter specified in the CPD file, which is set in the Site Administration user interface. It specifies the full path and file name of the FTP client.                                                                                                                                                                                                                                                                                                                            |
| -d        | debugfile              | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| -H        | hostname               | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ Value passed on the command line using the <b>-H</b> parameter</li> <li>◆ Value of the CMUHOST environment variable</li> <li>◆ Value of the gethostname() system call</li> <li>◆ Literal value of <i>localhost</i></li> </ul>                                                      |
| -l        | debug level            | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -j        | none                   | Specifies strict transmission rules are applied to batch separation if Separate concatenated file groups by mailbox ID=YES (in UI) or BCHSEP=OPT4 (in ACD file). If this parameter is enabled, batches must meet the following conditions before they are transmitted: <ul style="list-style-type: none"> <li>◆ batch is requestable</li> <li>◆ batch has not been transmitted and is not in the process of being transmitted</li> <li>◆ batch is not marked incomplete</li> <li>◆ batch has not been deleted</li> </ul> |



| Parameter | Value                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -K        | <i>n</i>               | Specifies the SO_KEEPALIVE option on the control socket. This setting only affects FTP and Secure FTP transmissions, and does not affect SSHFTP transmissions. The actual interval of transmission for the TCP KEEPALIVE packets is a operating system level variable and must be reviewed and changed by the host system administrator. If specific help is required for administration of the TCP KEEPALIVE interval, the customer should contact their operating system vendor for assistance.<br>Valid values:<br>0 - no keep alive is set<br>1 - keep alive for autoconnect only<br>2 - keep alive for remote connect only<br>3 - keep alive for both autoconnect and autoconnect |
| -L        | Port Listener for FTPD | Specifies the port the FTP server daemon monitors for connections. The default is specified in ftp.cpd. This parameter can be set using the <b>Listener Port</b> control in the Site Administration user interface. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root.                                                                                                                                                                                                                                                                                                   |
| -n        | <none>                 | Turns off server-side support for the FTP rename command. Clients logging in cannot issue a RENAME <i>oldfilename newfilename</i> command. For information on the RENAME command, refer to the <i>Standard FTP Commands</i> chapter of the <i>IBM Sterling Connect:Enterprise for UNIX Remote User's Guide</i> .                                                                                                                                                                                                                                                                                                                                                                       |
| -N        | <i>daemon Name</i>     | Overrides the default daemon name of FTP. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -P        | portno                 | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul>                              |

| Parameter | Value                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -p        | portno               | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail. |
| -Q        | nnnn                 | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. This value also sets the queue length for the ftp server port the remote client logs on to. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.                                                                            |
| -s        | ftpd server pathname | Overrides the <b>FTP server path</b> parameter specified in the CPD file. It specifies the full path and file name of the FTP server daemon.                                                                                                                                                                                                                                                                                                                                                                                                      |
| -S        | <none>               | Specifies to use FTP linked with SOCKS or SOCKS FTP (SOCKS support).<br>To inform the <b>cmuftp</b> daemon to use the FTP client that has SOCKS capabilities, users must start <b>cmuftp</b> with parameter <b>-S</b> . By default, <b>cmuftp</b> does not use the FTP client with SOCKS capabilities. All clients with SOCKS capabilities refer to the <i>/etc/socks.conf</i> file to navigate the SOCKS firewall. The <i>socks.conf</i> file contains information such as the host IP address, destination IP address, and so forth.            |
| -t        | nnnn                 | Specifies the FTP session timeout in seconds. Valid values are between 30 and 7200 seconds unless the -T parameter is defined. The default is 900.                                                                                                                                                                                                                                                                                                                                                                                                |
| -T        | nnnn                 | Specifies the maximum for the -t parameter and the top range for the SITE IDLE command. Value values are between 30 and 7200 seconds.                                                                                                                                                                                                                                                                                                                                                                                                             |

| Parameter | Value            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -x        | max FTP sessions | <p>Specifies the maximum number of FTP sessions (auto connect and remote connect) that can be running simultaneously in the system. The default is 20.</p> <p>Specify this value using the <b>Maximum number of current sessions</b> parameter on the Create a Schedule screen in the Site Administration user interface.</p> <p>If all the remote accounts listed in a single ACD are FTP remote accounts, you cannot set <b>Sessions</b> to a value greater than that specified with the FTP daemon <b>-x</b> parameter.</p> <p>If the list contains a mix of remote accounts using different protocols, <b>Sessions</b> can be effective in limiting the total number of simultaneous sessions for that auto connect to a value greater than the <b>-x</b> value for FTP.</p> <p>Unlike Async and Bisync, FTP is not limited by a finite number of physical ports. Each FTP session consumes system resources. If the <b>-x</b> parameter of the FTP daemon is set too high, any number of errors can be expected: shared memory errors, too many processes, too many open files, and so forth. When the number of simultaneous FTP sessions across all active auto connects and remote connects reaches the limit value specified with the FTP daemon <b>-x</b> parameter, the following message is posted to stderr:</p> <pre>ERROR: cmuftp - No of Sessions exceeded MAX_FTP_ SESSIONS (20) limit.</pre> <p>If this message occurs when an FTP auto connect is attempting to start the 21st session (assuming the default limit of 20), specifying a value greater than 0 in the <b>Requeues</b> parameter permits the failing session to be queued for a subsequent attempt.</p> <p>If <b>Requeues</b> was set to <b>0</b> in the ACD, the session fails without being queued.</p> <p>If this error occurs when the 21st FTP session is a remote connect, the FTP remote must retry. See the <b>Times to requeue remote resource field on the Create a Schedule screen in the Site Administration user interface.</b></p> |
| -? -h     |                  | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Modifying the Signon Banner

Use the following procedure to display a custom banner message to users signing on to the system:

1. From the \$CMUHOME/etc directory, open ceustartup.
2. Add the following line:

```
export CMUFTPBanner="Banner displayed to users"
```

where *Banner displayed to users* is the text you want displayed in your startup script.

You can use a different banner for each **cmuftp** instance by setting a value for each instance before the next instance is started.

3. Run **ceushutdown**.
4. Run **ceustartup**.

## cmusshftpd—SSH Daemon

The SSH daemon serves remote sites that use the SSHFTP protocol.

### cmusshftpd Parameters

The parameters for **cmusshftpd** are described in the following table:

| Parameter | Value                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -C        | CPD configuration file   | Overrides the default CPD file name. The default is <i>\$CMUHOME/cpd/ftp.cpd</i> .                                                                                                                                                                                                                                                                                                                                                                                                  |
| -c        | SSHFTP client pathname   | Overrides the SSHFTP <b>client path</b> parameter specified in the CPD file, which is set in the Site Administration user interface. It specifies the full path and file name of the SSHFTP client.                                                                                                                                                                                                                                                                                 |
| -d        | debugfile                | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -H        | hostname                 | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul> |
| -l        | debug level              | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -L        | Port Listener for SSHFTP | Specifies the port the SSHFTP server daemon monitors for connections. The default is specified in <i>sshftp.cpd</i> . This can be set using the <b>Listener Port</b> control in the Site Administration user interface. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root.                                                                                            |
| -N        | <i>daemon Name</i>       | Overrides the default daemon name of SSHFTP. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                            |

| Parameter | Value                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -P        | portno                     | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMU<code>PORT</code> environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a <code>getservbyname()</code> call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p        | portno                     | <p>Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to <code>stderr</code> and the daemon startup will fail.</p>                                                                                                                      |
| -Q        | nnnn                       | <p>Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. This value also sets the queue length for the <code>sshftp</code> server port the remote client logs on to. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems.<br/><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.</p>                                                                                                                                                                                             |
| -s        | sshftpd server<br>pathname | <p>Overrides the SSHFTP <b>server path</b> parameter specified in the CPD file. It specifies the full path and file name of the SSHFTP server daemon.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -t        | nnnn                       | <p>Specifies the SSHFTP session timeout in seconds. Valid values are between 30 and 7200 seconds unless the <code>-T</code> parameter is defined. The default is <b>900</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Parameter | Value               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -x        | max SSHFTP sessions | <p>Specifies the maximum number of SSHFTP sessions (auto connect and remote connect) that can be running simultaneously in the system. The default is 20. Specify this value using the <b>Maximum number of current sessions</b> parameter on the Create a Schedule screen in the Site Administration user interface.</p> <p>If all the remotes listed in a single ACD are SSHFTP remotes, you cannot set <b>Sessions</b> to a value greater than that specified with the SSHFTP daemon <b>-x</b> parameter.</p> <p>If the list contains a mix of remotes using different protocols, <b>Sessions</b> can be effective in limiting the total number of simultaneous sessions for that auto connect to a value greater than the <b>-x</b> value for SSHFTP.</p> <p>Unlike Async and Bisync, SSHFTP is not limited by a finite number of physical ports. Each SSHFTP session consumes system resources. If the <b>-x</b> parameter of the SSHFTP daemon is set too high, any number of errors can be expected: shared memory errors, too many processes, too many open files, and so forth. When the number of simultaneous SSHFTP sessions across all active auto connects and remote connects reaches the limit value specified with the SSHFTP daemon <b>-x</b> parameter, the following message is posted to stderr:</p> <pre>ERROR: cmusshftpd - No of Sessions exceeded MAX_SSHFTP_ SESSIONS (20) limit.</pre> <p>If this message occurs when an SSHFTP auto connect is attempting to start the 21st session (assuming the default limit of 20), specifying a value greater than 0 in the <b>Requeues</b> parameter permits the failing session to be requeued for a subsequent attempt.</p> <p>If <b>Requeues</b> was set to <b>0</b> in the ACD, the session fails without being requeued.</p> <p>If this error occurs when the 21st SSHFTP session is a Remote Connect, the SSHFTP remote must retry. See the <b>Times to requeue remote resource field on the Create a Schedule screen in the Site Administration user interface.</b></p> |
| -? -h     |                     | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

### cmubscda—Bisync Daemon for ARTIC Card

The ARTIC Bisync daemon serves remote sites using Bisync 3780 or 2780 protocols and synchronous modems. Auto connects using SADL, v.25bis, and AT Command Set autodialing modems are supported. Autodialing with 801C ACUs paired to synchronous modems is also supported with the use of two ports.

The debug tracing facility allows viewing of traces from separate Bisync ports. When tracing is enabled upon startup (through the **-d** and **-l** parameters), each port is assigned its own trace file based on the card and port coded in the CPD file. Whatever value is supplied through the **-d** parameter is used as a prefix to create a unique file name for each port. The master daemon is also given a unique name.

If you run **cmusession** immediately after **ceustartup**, the output of **cmusession** does not display the Bisync subsystem daemon. The Bisync daemon registers itself only after it has reset all the ARTIC cards in the system.

### cmubscda Parameters

All **cmubscda** parameters are optional. The parameters for **cmubscda** are described in the following table:

| Parameter | Value                  | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -C        | CPD configuration file | Instructs the Bisync daemon to use a specific CPD file. The default is bisynca.cpd in the <i>\$CMUHOME/cpd</i> directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| -d        | debugfile              | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -H        | hostname               | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l        | debug level            | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -N        | daemon name            | This parameter is required if you intend to run multiple copies of <b>cmubscda</b> . The <b>cmubscda</b> daemon uses the specified value as a name to register with the Control daemon. The default value for this parameter is BISYNC. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                       |
| -n        |                        | Indicates that the card is not reset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| -P        | portno                 | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |

| Parameter | Value                  | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -p        | portno                 | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail. |
| -Q        | nnnn                   | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development.                                                                                                                                                                        |
| -T        |                        | Must be specified when using the <i>rticbscp.exe</i> driver for a Multiport Model 2 card or a Portmaster card.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -X        | ARTIC device file name | If you installed the device driver as other than <i>/dev/artic</i> , you must invoke <b>cmubscda</b> with this option. For example: <code>cmubscda -X /dev/artic2</code> .                                                                                                                                                                                                                                                                                                                                                                        |
| -? -h     |                        | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

### cmubscdc—Bisync Daemon for Cleo SYNCcable+ Hardware

The Cleo Bisync daemon serves remote sites using Bisync 3780 protocols and, either the native asynchronous ports on your UNIX server, or a port server such as the Digi Etherlite port server from Cleo Communication Systems.

You must install and test the Cleo SYNCcable+ hardware and software according to the installation instructions provided by Cleo Communication Systems, Inc. before you configure Sterling Connect:Enterprise to use `cmubscdc`. This daemon is included as a comment line in the installed `ceustartup`. If you installed and tested the appropriate hardware, you can edit the startup script to call this daemon.

As mentioned in the Cleo Communication Systems, Inc. *3780Plus User's Guide*, a separate working directory must be established for every SYNCcable+ device in use.

| Command | Parameter              | Associated Values                                                                           |
|---------|------------------------|---------------------------------------------------------------------------------------------|
| -C      | CPD configuration file | Instructs the Bisync daemon to use a specific CPD file. The default is <i>bisyncc.cpd</i> . |
| -d      | debugfile              | Specifies the debug message output file name.                                               |



| Command | Parameter   | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -H      | hostname    | <p>Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is:</p> <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l      | debug level | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| -N      | daemon name | The default is BISYNC. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| -P      | portno      | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p      | portno      | <p>Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.</p>                                                                                                         |
| -Q      | nnnn        | <p>Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems.</p> <p><b>CAUTION:</b> Use this switch only when instructed to do so by IBM Support or Development.</p>                                                                                                                                                                                                                                                                            |
| -? -h   |             | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## cmuhttpd—HTTP Daemon for AS2

The HTTP daemon is a specialized HTTP daemon used for sending and receiving packaged AS2 messages. After the EDIINT daemon packages the messages, the HTTP daemon sends it. Incoming AS2 messages are received by the HTTP daemon and passed to the EDIINT daemon for unpackaging. By default, this daemon is commented out. Remove the comment markers before running the startup script.

| Command | Parameter   | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -c      | Classpath   | Specifies the location of your class files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| -d      | debugfile   | Specifies the debug message output file name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| -H      | hostname    | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l      | debug level | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -N      | daemon name | The default is HTTP. Do not change the default value if you use the Site Administration user interface. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| -P      | portno      | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p      | portno      | Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.                                                                                                         |

| Command | Parameter    | Associated Values                                                                                                                                                                                                                                                                                                                                                          |
|---------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -Q      | nnnn         | Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems.<br><i>CAUTION:</i> Use this switch only when instructed to do so by IBM Support or Development. |
| -x      | max sessions | Specifies the maximum number of HTTP sessions that are supported. The default value is 20.                                                                                                                                                                                                                                                                                 |
| -h      |              | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                |

### Timeout for the HTTP Daemon

The HTTP daemon has a default timeout of 10 seconds (10000 ms). This value denotes the amount of time each socket read will wait to complete before an error occurs. For more information on this default timeout value, access [http://www.java.net.Socket.setTimeout\(\)](http://www.java.net.Socket.setTimeout()). The value can be changed by setting the `com.sterlingcommerce.ceu.http.listenerTimeout` value in the `ceuhhttpd` script as shown in the following example:

```
listenerTimeout="-Dcom.sterlingcommerce.ceu.http.listenerTimeout=100000"
```

This will set the timeout value to 100000 milliseconds (100 seconds).

---

**Note:** Do not set this value to zero (0). If you do, it will disable the read timeout and cause problems.

---

### cmuediintd—EDIINT Daemon for AS2

The EDIINT daemon is used to package AS2 messages before sending them and to unpackage incoming AS2 messages before forwarding to the destination mailbox. Remove the comment markers before running the startup script.

| Command | Parameter | Associated Values                             |
|---------|-----------|-----------------------------------------------|
| -c      | Classpath | Specifies the location of your class files.   |
| -d      | debugfile | Specifies the debug message output file name. |

| Command | Parameter    | Associated Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -H      | hostname     | <p>Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is:</p> <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -l      | debug level  | Specifies the debug message level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| -N      | daemon name  | The default is EDIINT. Do not change the default value if you use the Site Administration user interface. Daemon names should be 8 characters or less with no spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| -P      | portno       | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p      | portno       | <p>Specifies the port this daemon will monitor for inter-process communication. If NOT specified, the daemon will request a random port from the operating system and monitor it. Typical setting is a value greater than 1024. If a port number of 1 to 1024 is used, special system privileges are required because the daemon must run as root. If the port number is specified, the daemon will attempt to request exclusive use of that port. If it cannot get it, an error message will be written to stderr and the daemon startup will fail.</p>                                                                                                         |
| -Q      | nnnn         | <p>Enables you to modify the listener socket queue length so that inter-process messages to this daemon are not lost during periods of high activity. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems.</p> <p><b>CAUTION:</b> Use this switch only when instructed to do so by IBM Support or Development.</p>                                                                                                                                                                                                                                                                            |
| -x      | max sessions | Specifies the maximum number of EDIINT sessions that are supported. The default value is 20.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

---

## Shutting Down Sterling Connect:Enterprise

While individual parts of Sterling Connect:Enterprise can be stopped independently, sometimes you need to bring the entire system down. This is accomplished with the **ceushutdown** command.

### ceushutdown Format

To request an orderly shutdown of Sterling Connect:Enterprise, enter the following command:

```
ceushutdown
```

### ceushutdown Output

**System Down** is displayed after all components of the system are successfully shut down.

### ceushutdown Parameters

Parameters for **ceushutdown** can be typed using either the abbreviated or long format.

The abbreviated parameters, those beginning with a single hyphen, can be separated from their associated values by a space or the values can immediately follow without separation.

The long parameters, those beginning with two hyphens, *must* be separated from their associated values with either a space or an equal sign.

All **ceushutdown** parameters are optional. Unless otherwise noted, the parameters apply to all environments.

| Parameter    | Value    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -H<br>--host | hostname | Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul> |

| Parameter         | Value    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -i<br>--immediate |          | Changes the method Sterling Connect:Enterprise uses to shut down the system. Usually, Sterling Connect:Enterprise shuts down the system gradually, daemon by daemon, in an orderly fashion. New connections are not enabled, but each daemon is allowed to end its current sessions before shutting down. After all of the daemons are shut down, the Control daemon shuts down the Utility daemons, then finally itself. If -i is specified, all daemons are notified to shutdown. Current sessions may or may not complete.                                                                                                                             |
| -P<br>--port      | portno   | Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows: <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |
| -p<br>--passwd    | password | Specifies the value within Sterling Connect:Enterprise associated with the current user name. If the default value for -u username is used, the password is matched to that user name-defined password within Sterling Connect:Enterprise.                                                                                                                                                                                                                                                                                                                                                                                                                |
| -u<br>--user      | username | Enables multiple user names to log on to the UNIX host. Its use is optional because the command utilities obtain the user's name from the system as a default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| -?<br>--help      |          | Displays the usage message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Shutting Down Sterling Connect:Enterprise Base

Shutting down Sterling Connect:Enterprise base is accomplished with the **cmshutdown** command.

### cmshutdown Format

To request an orderly shutdown of Sterling Connect:Enterprise base, enter the following command:

```
cmshutdown
```

## cmushutdown Parameters

Parameters for **cmushutdown** can be typed using either the abbreviated or long format.

The abbreviated parameters, those beginning with a single hyphen, can be separated from their associated values by a space or the values can immediately follow without separation.

The long parameters, those beginning with two hyphens, *must* be separated from their associated values with either a space or an equal sign.

All **cmushutdown** parameters are optional. Unless otherwise noted, the parameters apply to all environments.

| Parameter         | Value    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -H<br>--host      | hostname | <p>Specifies the IP address or host name where the Control daemon is executing. Sterling Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is:</p> <ul style="list-style-type: none"> <li>◆ The value passed on the command line using the <b>-H</b> parameter</li> <li>◆ The value of the CMUHOST environment variable</li> <li>◆ The value of the gethostname() system call</li> <li>◆ The literal value of <i>localhost</i></li> </ul>                                                                                                                                                                       |
| -i<br>--immediate |          | <p>Changes the method Sterling Connect:Enterprise uses to shut down the system. Usually, Sterling Connect:Enterprise shuts down the system gradually, daemon by daemon, in an orderly fashion. New connections are not enabled, but each daemon is allowed to end its current sessions before shutting down. After all of the daemons are shut down, the Control daemon shuts down the Utility daemons, then finally itself. If <b>-i</b> is specified, all daemons are notified to shutdown. Current sessions may or may not complete.</p>                                                                                                                      |
| -P<br>--port      | portno   | <p>Specifies the port the Control daemon monitors. If <b>-P</b> is NOT specified on the command line, the value of the CMUPORT environment variable is used, if it exists. Regardless of the source of the value, the value is evaluated as follows:</p> <ul style="list-style-type: none"> <li>◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number.</li> <li>◆ If the value does not begin with a digit, a getservbyname() call is made to attempt to resolve the given service name to a port number.</li> <li>◆ If these two tests fail, the default value of 8000 is used.</li> </ul> |

| <b>Parameter</b> | <b>Value</b> | <b>Description</b>                                                                                                                                                                                                                         |
|------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -p<br>--passwd   | password     | Specifies the value within Sterling Connect:Enterprise associated with the current user name. If the default value for -u username is used, the password is matched to that user name-defined password within Sterling Connect:Enterprise. |
| -u<br>--user     | username     | Enables multiple user names to log on to the UNIX host. Its use is optional because the command utilities obtain the user's name from the system as a default.                                                                             |
| -?<br>--help     |              | Displays the usage message.                                                                                                                                                                                                                |



---

# Role-Based Access

This chapter provides information on designing your role-based access system for the Sterling Connect:Enterprise for UNIX Site Administration user interface. Read this information and perform the procedures described in this chapter before attempting to implement a role-based access system using the Site Administration user interface.

---

## About Role-Based Access

Role-based access enables you to create predefined sets of system permissions available from the Sterling Connect:Enterprise Site Administration user interface. These are called roles. You then assign users of the Site Administration user interface to these roles. When a user logs on, the items in the navigation bar are determined by the permissions available to the user's role. All users of the Sterling Connect:Enterprise for UNIX Site Administration user interface must be assigned to a role.

Sterling Connect:Enterprise is installed with a single active role: Administrator. The Administrator role has access to all resources and is the parent of all roles that you create. You cannot change anything about the Administrator role. The userID assigned during installation is associated with the Administrator role.

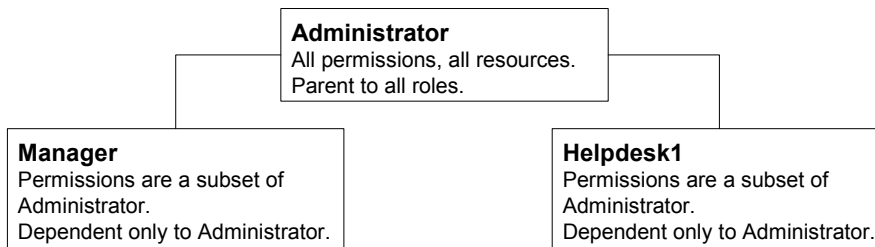
You can set up a single-level role-based access system in which roles operate independently of each other. You can also set up a multilevel role-based access system to create a hierarchy of permission levels.

---

## Designing a Single-Level Role-Based Access System

A single-level system has only two permission levels. The first is Administrator, which contains all permissions for all resources and roles. The second level contains all other roles. The second-level roles are resources only of the Administrator role, and the Administrator role is the only parent role.

The following diagram illustrates a single-level role-based access system:



To create a single-level role-based access system, use the following procedure:

1. Identify a set of resource permissions to include in the role. Refer to *Resource Permissions* on page 108 for a list of resource permissions you can specify.
2. Decide on a role name for this group of resource permissions, such as Manager or Helpdesk1.
3. List the user accounts that will be assigned to the role.
4. Repeat steps 1-3 until you have identified resource permissions, names, and account lists for all roles. Be certain that you have all users that will use the Site Administration user interface assigned to a role. The following example shows what role definitions for a single level role-based access system would include:

|                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Role Name: <b>Manager</b></p> <p><u>Resource Permissions</u></p> <p>Data Management - Modify</p> <p>Reports - View</p> <p><u>Role Permissions</u></p> <p>None</p> <p><u>Accounts Assigned to Role</u></p> <p>user01-mgr</p> <p>user02-mgr</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Role Name: <b>Helpdesk1</b></p> <p><u>Resource Permissions</u></p> <p>Accounts - Administer</p> <p>Data - Administer</p> <p>Password - Administer</p> <p>Policy - View</p> <p>Reports - View</p> <p>Role-Based-Access - Administer</p> <p>Schedule - Administer</p> <p>Security - View</p> <p>System - View</p> <p><u>Role Permissions</u></p> <p>None</p> <p><u>Accounts Assigned to Role</u></p> <p>user03</p> <p>user04</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

5. Use the **Define Roles** function in the Sterling Connect:Enterprise for UNIX Site Administration user interface to create the roles and assign accounts to each role.

---

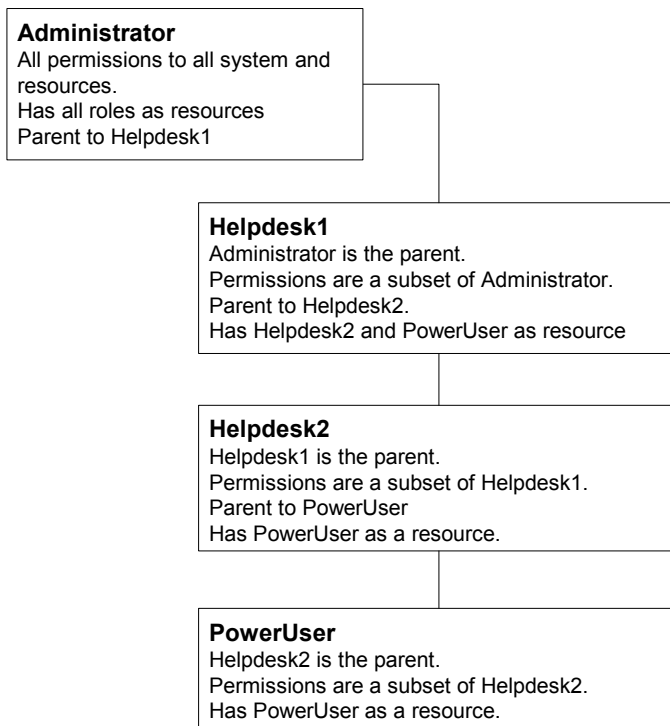
**Note:** When using the interface to design a single-level role-based access system, you will need to disable all role permissions on the Assign Role Permissions screen.

---

## Designing a Multilevel Role-Based Access System

You can create a multilevel role-based access system that uses various levels of permissions with a parent-dependent relationship between one or more roles. This enables you to create a hierarchy of permissions.

The following example illustrates a multilevel role-based access system:



To create a multilevel role-based access system, use the following procedure:

1. Identify a set of resource permissions that you will include in the highest level role next to Administrator. Refer to *Resource Permissions* on page 108 for a list of resource permissions you can specify.
2. In a multilevel role-based access system, roles can have permissions on other roles. Identify what permissions you want the role you are creating to have to act on other roles. Refer to *Role Permissions* on page 110 for a list of role permissions.
3. Decide on a role name for this group of resource permissions, such as Manager or Helpdesk1.
4. List the user accounts that will be assigned to the role.
5. Identify the role for which you want to create a dependent role and decide on a name for the dependent role. In this example, Helpdesk2 is created as a dependent of Helpdesk1.
6. Identify a set of resource permissions that you will include in the next level role. Refer to *Resource Permissions* on page 108 for a list of resource permissions you can specify. A

dependent role cannot have any permissions that the parent does not have. In this example, you determine the resource permissions Helpdesk2 inherits from Helpdesk1.

7. Identify a set of role permissions that you will include in the next level role. Refer to *Role Permissions* on page 110 for a list of role permissions you can specify. A dependent role cannot have any permissions that the parent does not have. In this example, you determine the role permissions Helpdesk2 inherits from Helpdesk1.
8. List the user accounts to be assigned to the dependent role.

You can create additional levels by repeating steps step 1 on page 107-step 8 on page 108. Following is an example of what role definitions for a multi-level role-based access system would include:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role Name: <b>Helpdesk1</b><br>Parent Role: <b>Administrator</b><br><u>Resource Permissions</u><br>Accounts - Administer<br>Data - Administer<br>Password - Administer<br>Policy - Administer<br>Reports - Administer<br>Role-Based-Access - Administer<br>Schedule - Administer<br>Security - View<br>System - View<br><u>Role Permissions</u><br>Helpdesk1 - View, Associate<br>Helpdesk2 - All<br>PowerUser - All<br><u>Accounts Assigned to Role</u><br>user03<br>user04 | Role Name: <b>Helpdesk2</b><br>Parent Role: <b>Helpdesk1</b><br><u>Resource Permissions</u><br>Accounts - View<br>Data - Administer<br>Password - Administer<br>Policy - Administer<br>Reports - View<br>Role-Based-Access - View<br>Schedule - Execute<br>Security - View<br>System - View<br><u>Role Permissions</u><br>Helpdesk2 - View, Associate<br>PowerUser - All<br><u>Accounts Assigned to Role</u><br>user05<br>user06 | Role Name: <b>PowerUser</b><br>Parent Role: <b>Helpdesk2</b><br><u>Resource Permissions</u><br>Accounts - View<br>Data - Administer<br>Reports - View<br>Schedule - Execute<br>Security - View<br>System - View<br><u>Role Permissions</u><br>PowerUser - View, Associate<br><u>Accounts Assigned to Role</u><br>user07<br>user08 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

When a dependent role is created, it becomes a dependent of all roles above it in the hierarchy. In this example, PowerUser is a dependent of both Helpdesk2 and Helpdesk1.

9. Use the **Define Roles** function in the Sterling Connect:Enterprise Site Administration user interface to create the roles and assign accounts to each role.

---

## Resource Permissions

The following table contains the list of resources for which you can assign permissions and a description of each permission level:

| Resource | Permission Level | Description                                                                       |
|----------|------------------|-----------------------------------------------------------------------------------|
| Accounts | Administer       | Users assigned to the role can view, add, update, and delete account information. |

| Resource        | Permission Level | Description                                                                                                                                                                                                               |
|-----------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | View             | Users assigned to the role can view account information, but cannot add, update, or delete.                                                                                                                               |
|                 | Delegate         | Users assigned to the role can delegate account permissions to roles they are parent to.                                                                                                                                  |
| AS2             | Administer       | Users assigned to the role can view, add, update, and delete AS2 communications, proxy, and contract information.                                                                                                         |
|                 | View             | Users assigned to the role can only view AS2 communications, proxy, and contract information.                                                                                                                             |
|                 | Delegate         | Users assigned to the role can delegate AS2 communications, proxy, and contract information to roles they are parent to.                                                                                                  |
| AS2 Report      | View             | Users assigned to the role can generate AS2 reports.                                                                                                                                                                      |
| Communications  | Administer       | Users assigned to the role can view, add, update, and delete communication protocol information.                                                                                                                          |
|                 | View             | Users assigned to the role can view communication data but cannot add, update, or delete communication protocol information.                                                                                              |
|                 | Delegate         | Users assigned to the role can delegate Communications permissions to roles they are parent to.                                                                                                                           |
| Data Management | Administer       | Users assigned to the role can view, modify, erase, delete, erase, extract batches, view system status, and view the contents of a batch. User can also delegate Data Management permissions to roles they are parent to. |
|                 | View             | Users assigned to the role can view batch information, but cannot update or delete batch information.                                                                                                                     |
|                 | Delegate         | Users assigned to the role can delegate Data Management permissions to roles they are parent to.                                                                                                                          |
|                 | Modify           | Users assigned to the role can modify batches in the repository.                                                                                                                                                          |
|                 | Erase            | Users assigned to the role can physically delete batches from the repository.                                                                                                                                             |
|                 | Delete           | Users assigned to the role can mark batches in the repository to be deleted.                                                                                                                                              |
|                 | Extract          | Users assigned to the role can extract batches in the repository to a file.                                                                                                                                               |
| Password        | Administer       | Users assigned to the role can reset another user's password.                                                                                                                                                             |
| Policy          | Administer       | Users assigned to the role can create, update, and delete password policies.                                                                                                                                              |
| Reports         | View             | Users assigned to the role can generate Sterling Connect:Enterprise reports.                                                                                                                                              |

| Resource          | Permission Level | Description                                                                                                               |
|-------------------|------------------|---------------------------------------------------------------------------------------------------------------------------|
| Role-Based Access | Administer       | Users assigned to the role can view role details and add, update, or delete roles.                                        |
|                   | View             | Users assigned to the role can view role details but cannot add, update, or delete roles.                                 |
|                   | Delegate         | Users assigned to the role can delegate Role permissions to roles they are parent to.                                     |
| Schedule          | Administer       | Users assigned to the role can view schedule details and add, update, and delete schedules.                               |
|                   | View             | Users assigned to the role can view schedule details but cannot add, update, or delete schedules.                         |
|                   | Delegate         | Users assigned to the role can delegate schedule permissions to roles they are parent to.                                 |
|                   | Execute          | Users assigned to the role can run a schedule manually.                                                                   |
| Security          | Administer       | Users assigned to the role can view security policy details and add, update, and delete security policies.                |
|                   | View             | Users assigned to the role can view security policy details but cannot add, update, or delete security policies.          |
|                   | Delegate         | Users assigned to the role can delegate security policy permissions to roles they are parent to.                          |
| System            | Administer       | Users assigned to the role can view system configuration details and add, update, and delete the system configuration.    |
|                   | View             | Users assigned to the role can view system configuration details but cannot add, update, or delete system configurations. |
|                   | Delegate         | Users assigned to the role can delegate system configuration permissions to roles they are parent to.                     |

## Role Permissions

Role permissions are the permissions a role is given to operate on other roles. The following table contains the list of role permissions and a description of each permission level:

| Permission Level | Description                                                                     |
|------------------|---------------------------------------------------------------------------------|
| View             | Users assigned to the role can view the properties of the role resource.        |
| Update           | Users assigned to the role can view and update properties of the role resource. |

---

| <b>Permission Level</b> | <b>Description</b>                                                           |
|-------------------------|------------------------------------------------------------------------------|
| Delete                  | Users assigned to the role can delete the role resource.                     |
| Associate               | Users assigned to the role can assign the role resource to additional roles. |

---





---

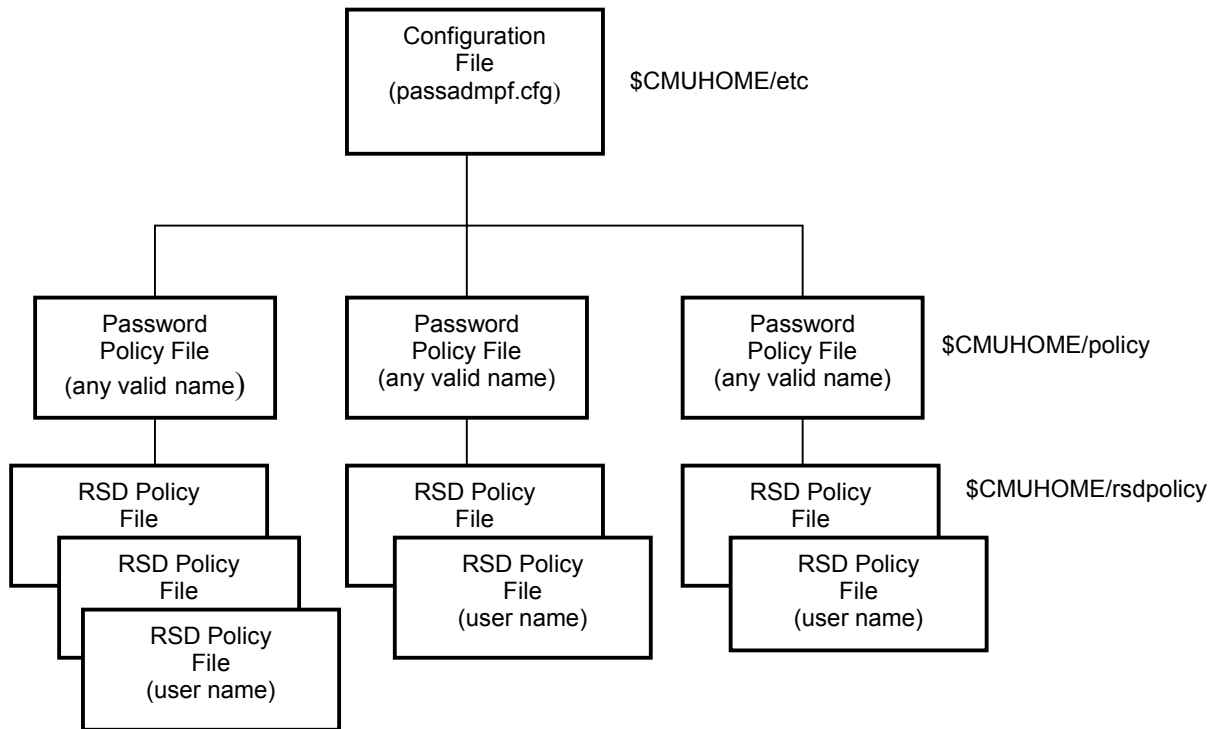
# Password Administration

The password administration feature enables you to create one or more password policy definitions (policy files). Policy files define the number of days a password is valid, the number of consecutive failed logon attempts allowed, the maximum and minimum password length, and the number of entries in a password history file. You can use the values in password policy files to manage the password characteristics of the individual account files (remote site definition files) used to authenticate local or protocol connections to Sterling Connect:Enterprise for UNIX. Outbound RSD (remote site definition blocks) behavior is unaffected by password policy files.

You can define policy files using the offline utilities described in this chapter or the Sterling Connect:Enterprise Site Administration user interface described in Chapter 1, *About Sterling Connect:Enterprise for UNIX*. Policy files describe the password characteristics that you apply to a user's RSD policy file.

RSD policy files contain the password policy implementation specifics for a given account (RSD file). These files contain the absolute password expiration date, maximum consecutive logon attempts, current consecutive failed logon attempts, password history, minimum and maximum password length, and the name of the associated policy file.

The following figure illustrates the relationship of the password policy configuration file, password policy files, and the RSD policy files for user accounts.




---

## Configuration File

By default, the password administration feature is not enabled. The following example illustrates the default password administration configuration file, `$CMUHOME/etc/passadmpf.cfg`. To implement password administration, you set the values for the `POLICY_LEVEL=` parameter and the `EMAIL=` parameter in the configuration file using a text editor, for example `vi`.

```

EMAIL=host:port/support@ceunix.customer.com
POLICY_LEVEL=0

CONSECUTIVE_FAILED_LOGON_FLAG=N
DURATION_FLAG=N
PASSWORD_HISTORY_FLAG=N
PASSWORD_LENGTH=N

CONSECUTIVE_FAILED_LOGON_ATTEMPTS=5
DURATION=366
MAXIMUM_PASSWORD_LENGTH=64
MINIMUM_PASSWORD_LENGTH=1
PASSWORD_HISTORY=5
  
```

The following table describes the parameters that enable password administration and their valid values. You can define these parameters only in the password configuration file.

| Parameter     | Description                                                                                                                  | Value                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMAIL=        | Specifies the e-mail address of the person to notify when an account is locked because of consecutive failed logon attempts. | Any valid e-mail address in the following format:<br>host:port/support@ceunix.customer.com                                                                                                                                                                         |
| POLICY_LEVEL= | Specifies how the system uses password policies. To use password administration, you must change this value to 1 or 2.       | 0 = Disallowed; RSD policy files are not evaluated. This is the default.<br>1 = Optional; If the RSD policy file exists for the user, it is evaluated.<br>2 = Required; All users who log on to Sterling Connect:Enterprise for UNIX must have an RSD policy file. |

You also define the default values for a password policy or policies in the configuration file by updating the remaining configuration file default values. However, when you create a new password policy, you can override all the default values except those for EMAIL= and POLICY\_LEVEL=. See *Creating and Maintaining Password Policy Files* on page 116 for a complete description of the configuration file parameters.

## Password Policy Files

You create two types of password files: system policy files and RSD policy files. System policy files contain the rules for generating an RSD policy file for an individual account. You can create multiple password policy files. A policy file contains the default values from the configuration file and any overrides specified when you create it. A policy file can have any valid UNIX file name. The following example illustrates the password policy file \$CMUHOME/policy/policy1.

```
DURATION_FLAG=Y
DURATION=30
CONSECUTIVE_FAILED_LOGON_FLAG=Y
CONSECUTIVE_FAILED_LOGON_ATTEMPTS=3
PASSWORD_HISTORY_FLAG=Y
PASSWORD_HISTORY=3
PASSWORD_LENGTH=Y
MINIMUM_PASSWORD_LENGTH=1
MAXIMUM_PASSWORD_LENGTH=64
FORCED_EXPIRATION_FLAG=N
FORCED_EXPIRATION_DATE= N
CHANGE_PASSWORD_FLAG=Y
HASH=588D2C9CFE24074452EB68B996D5D492667CDFFD
```

## RSD Policy Files

The RSD policy file is generated when you apply a password policy to an account (RSD file). Each user account (RSD) can have only one associated RSD policy file. Depending on the value set for the `POLICY_LEVEL=` parameter in the `passadmpf.cfg` file, some or all users require an RSD policy file. The RSD policy file name is the user's logon ID, which is also the name of the user's RSD file.

The following example illustrates the RSD policy file (`$CMUHOME/rsdpolicy/user1`) generated when *policy1* is applied to the account *user1*.

```
LOCKED=N
PASSWORD_CHANGE_REQUIRED=N
LOCK_REASON=
POLICY_FILENAME=policy1
PASSWORD_EXPIRATION=01/30/2003
WARNING_DAYS=10
MAX_CONSECUTIVE_LOGON_FAILURES=3
CONSECUTIVE_LOGON_FAILURES=0
PASSWORD_HISTORY=34FB6E9DB0F02DF3C0841FF41FA4F3926CBC7AF8
HISTORY_COUNT=1
HISTORY_MAX=3
MAX_PWD_LEN=64
MIN_PWD_LEN=1
DURATION=1
CHANGE_PASSWORD_FLAG=1
HASH=E3C72D704610CF97E54BE2C57247B344E641787A
```

Note that both the password policy file (see `DURATION_FLAG=Y` on page 115) and the RSD policy file generated by applying it to an account contain a `HASH=` value. This hash value prevents the files from being changed by any program other than the Sterling Connect:Enterprise offline password utilities or the Sterling Connect:Enterprise Site Administration user interface. Also note that this hash value includes the password from the user's RSD file.

If the RSD policy file or the user's password in the RSD file is changed by any program other than the Sterling Connect:Enterprise utilities or the Sterling Connect:Enterprise Site Administration user interface, the user is not allowed to log on, and the RSD policy file must be deleted and regenerated before the user can log on.

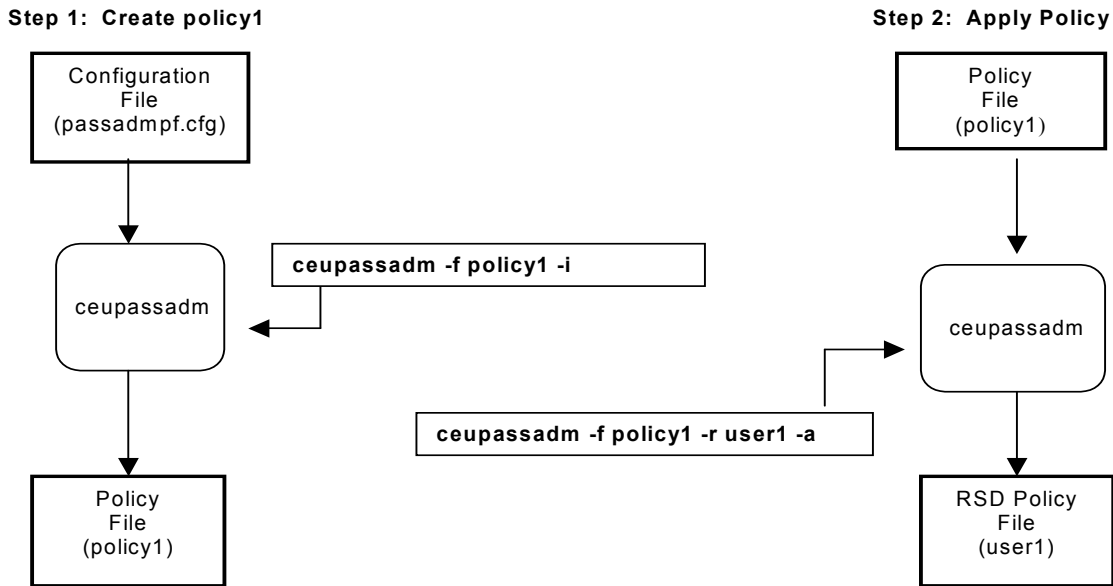
---

## Creating and Maintaining Password Policy Files

Three offline commands enable you to create and maintain password policy files, RSD policy files, and RSD files:

| Command/Utility         | Description                                                       |
|-------------------------|-------------------------------------------------------------------|
| <code>ceupassadm</code> | Creates and maintains password policy files and RSD policy files. |
| <code>ceupassrpt</code> | Displays RSD policy files.                                        |
| <code>ceupasswd</code>  | Enables users to change their password.                           |

The following illustration shows the flow associated with using **ceupassadm** to create a password policy and apply it to an account, which generates the RSD policy file for that account. In this illustration, the password policy uses the default values from the password configuration file (`passadmpf.cfg`).



The **ceupassadm** command accepts the parameters listed in the tables beginning on page 117.

| Parameter                | Description                            | Value                     |
|--------------------------|----------------------------------------|---------------------------|
| <code>-f filename</code> | Specifies policy file name to process. | Any valid UNIX file name. |
| <code>--file</code>      |                                        |                           |

| Parameter                                              | Description                                                                                                                                                                                                            | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -F<br>--Flags                                          | Sets control flags within a policy file.                                                                                                                                                                               | Any combination of the following flags:<br>N = No password controls; ignore all other flags.<br>X = Expiration date is active.<br>x = Expiration date is not active.<br>L = Maximum number of consecutive failed logon attempts is active.<br>I = Maximum number of consecutive failed logon attempts is not active.<br>H = History file is active.<br>h = History file is not active.<br>M = Min/Max password length is active.<br>m = Min/Max password length is not active.<br>E = Forced expiration is active.<br>e = Forced expiration is not active. |
| -d <i>ddd</i><br>--days <i>ddd</i>                     | Specifies the number of days before password expires. Passwords are valid until midnight of the password expiration date. Time and date are determined by the host system where the authentication service is running. | Valid values are 1–366.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -l <i>nnn</i><br>--logons <i>nnn</i>                   | Specifies the maximum number of consecutive logon failures before the account is locked.                                                                                                                               | Valid values are 1–999.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -s <i>nn</i><br>--save <i>nn</i>                       | Specifies the number of saved passwords in the password history file used for password change validation.                                                                                                              | Valid values are 1–99.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| -m <i>nn</i><br>--max <i>nn</i>                        | Specifies the maximum number of characters allowed in the password.                                                                                                                                                    | Valid values are 1–64.<br>Must be greater than or equal to the minimum password value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| -n <i>nn</i><br>--number <i>nn</i>                     | Specifies the minimum number of characters required in the password.                                                                                                                                                   | Valid values are 1–64.<br>Must be less than or equal to the maximum password value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -e <i>mm/dd/yyyy</i><br>--expiration <i>mm/dd/yyyy</i> | Sets the absolute password expiration date.                                                                                                                                                                            | Specify the year in four digits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| -i<br>--insert                                         | Creates a new policy file.                                                                                                                                                                                             | None.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

The following parameters apply only to RSD policy files:

| Parameter                                                | Description                                                                                                                                                                                                                            | Value                                                                                                                        |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| -r <i>rsdpolicy_filename</i><br>--rsdpolicy              | Specifies the RSD policy file to process.                                                                                                                                                                                              | Any valid RSD policy file name.                                                                                              |
| -L TRUE   FALSE<br>--Lock                                | Specifies the value of the RSD lock flag.                                                                                                                                                                                              | Valid value is TRUE or FALSE; default is FALSE. When set to TRUE, this lock forces the account inactive.                     |
| -w <i>nnn</i><br>--warning <i>nnn</i>                    | Specifies the number of days prior to the password expiration date to warn the user that his or her password will expire. After each successful logon, the following message is displayed:<br><i>Password will expire in nnn days.</i> | Valid values are 1–30.                                                                                                       |
| -C TRUE   FALSE<br>--Change                              | Specifies whether the user must change password at first logon.                                                                                                                                                                        | Valid values are TRUE or FALSE; default is FALSE.                                                                            |
| -S <i>newpassword</i><br>--Specify<br><i>newpassword</i> | Assigns a new password to the account.                                                                                                                                                                                                 | Any valid password.                                                                                                          |
| -a<br>--apply                                            | Applies the password policy to the RSD file.                                                                                                                                                                                           | None.                                                                                                                        |
| -b <i>bulk_filename</i><br>--bulk <i>filename</i>        | Specifies the name of a text file, called a bulk file, that contains a list of accounts (RSD files) to be associated with a password policy.                                                                                           | Any valid file name.<br>Use with the -a option to apply a password policy and generate the RSD policy file for the accounts. |

The following parameters apply to both policy files and RSD policy files:

| Parameter       | Description                        | Value |
|-----------------|------------------------------------|-------|
| ?, -h<br>--help | Lists command line options (help). | None. |
| -x<br>--delete  | Deletes the specified file.        | None. |

## Creating a Password Policy

The following command creates a password policy file called *myPolicy* with the following attributes:

- ◆ Password lifetime = 120 days
- ◆ Password history file = 6

- ◆ Lock value = 5 consecutive logon failures
- ◆ Maximum password length = 24 characters
- ◆ Minimum password length = 6 characters
- ◆ Absolute expiration date = 10/20/2003

```
ceupassadm -f myPolicy -F XLHME -d 120 -l 5 -s 6 -m 24 -n 6 -e 10/20/2003 -i
```

The following example illustrates the contents of *myPolicy*.

```
myPolicy: Policy file has been created
The policy file "myPolicy" contains the following:
DURATION_FLAG=Y
DURATION=120
CONSECUTIVE_FAILED_LOGON_FLAG=Y
CONSECUTIVE_FAILED_LOGON_ATTEMPTS=5
PASSWORD_HISTORY_FLAG=Y
PASSWORD_HISTORY=6
PASSWORD_LENGTH=Y
MINIMUM_PASSWORD_LENGTH=6
MAXIMUM_PASSWORD_LENGTH=24
CHANGE_PASSWORD_FLAG=Y
FORCE_EXPIRATION_DATE_FLAG=Y
FORCE_EXPIRATION_DATE=10/20/2003
This is the end of the policy file
```

## Forcing Password Change at Logon

The following command forces a user to change his or her password at first logon:

```
ceupassadm -r myRSD -C TRUE -a
```

The resulting RSD policy file is:

```
myRSD: RsdPolicy file has been modified.
The rsdpolicy file "myRSD" contains the following:
LOCKED=N
PASSWORD_CHANGE_REQUIRED=Y
LOCK_REASON=
POLICY_FILENAME=kmoor1Policy
PASSWORD_EXPIRATION=3/6/2003
WARNING_DAYS=10
MAX_CONSECUTIVE_LOGON_FAILURES=5
CONSECUTIVE_LOGON_FAILURES=0
This is the end of the rsdpolicy file
```



## Displaying Policy File Contents

The following command displays the contents of the policy file named *policy1*:

```
ceupassadm -f policy1
```

The result is:

```
The policy file "policy1" contains the following:
DURATION_FLAG=N
DURATION=366
CONSECUTIVE_FAILED_LOGON_FLAG=N
CONSECUTIVE_FAILED_LOGON_ATTEMPTS=999
PASSWORD_HISTORY_FLAG=N
PASSWORD_HISTORY=99
PASSWORD_LENGTH=N
MINIMUM_PASSWORD_LENGTH=1
MAXIMUM_PASSWORD_LENGTH=64
CHANGE_PASSWORD_FLAG=N
FORCE_EXPIRATION_DATE_FLAG=N
FORCE_EXPIRATION_DATE=
```

## Applying All Password Flags

The following command turns on all flags in the *policy1* password policy file:

```
ceupassadm -f policy1 -F XLHME -i
```

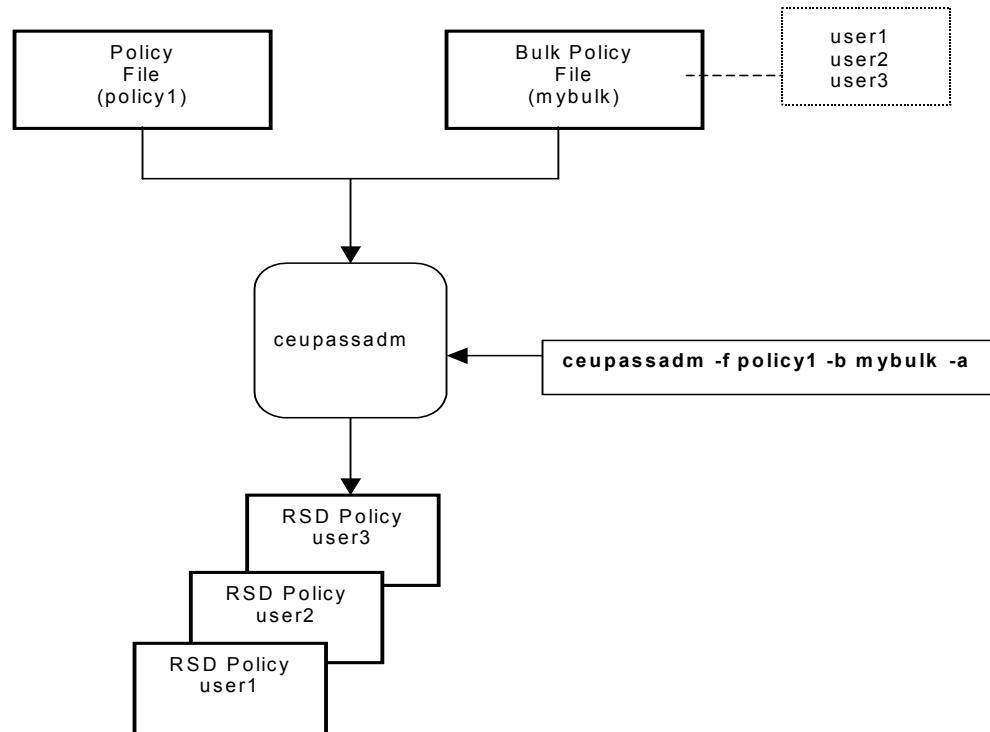
The resulting *policy1* file is:

```
policy1: Policy file has been modified.
The policy file "policy1" contains the following:
DURATION_FLAG=Y
DURATION=366
CONSECUTIVE_FAILED_LOGON_FLAG=Y
CONSECUTIVE_FAILED_LOGON_ATTEMPTS=999
PASSWORD_HISTORY_FLAG=Y
PASSWORD_HISTORY=99
PASSWORD_LENGTH=Y
MINIMUM_PASSWORD_LENGTH=1
MAXIMUM_PASSWORD_LENGTH=64
CHANGE_PASSWORD_FLAG=N
FORCE_EXPIRATION_DATE_FLAG=Y
FORCE_EXPIRATION_DATE=
This is the end of the policy file
```

## Applying a Password Policy to a Bulk File

You can apply a policy file to multiple account files using the bulk file option. Create a text file, called a bulk policy file, that contains the names of the accounts that you want to apply a password policy to and place the bulk file in the \$CMUHOME/bulkpolicy directory. As the following

diagram illustrates, applying the *policy1* file to the bulk file generates the RSD policy files for all accounts listed in the bulk file.



## Generating RSD Policy Reports

The **ceupassrpt** utility displays RSD policy files. You can select and display RSD policy files based on their expiration date or based on the password policy that generated them. The following table describes the **ceupassrpt** command line parameters.

| Parameter                                                             | Description                             | Value                                                           |
|-----------------------------------------------------------------------|-----------------------------------------|-----------------------------------------------------------------|
| -r <i>rsdpolicy_filename</i><br>--rsdpolicy <i>rsdpolicy_filename</i> | Specifies the RSD policy file name.     | Required; can be fully qualified or use wildcard character (*). |
| -e <i>mm/dd/yyyy</i><br>--expiration <i>mm/dd/yyyy</i>                | Specifies the password expiration date. | Optional; date on or before password expires.                   |

| Parameter                                                             | Description                              | Value                                                   |
|-----------------------------------------------------------------------|------------------------------------------|---------------------------------------------------------|
| -p <i>pwdpolicy_filename</i><br>--pwdpolicy <i>pwdpolicy_filename</i> | Specifies the password policy file name. | Optional; password policy that governs this RSD policy. |
| ?,-h<br>--help                                                        | Lists command line options (help).       | None.                                                   |

The following examples illustrate various ways to select and display RSD policy files:

- ◆ Display the RSD policy file *user1*:

```
ceupassrpt -r user1
```

The system displays the basic contents of the RSD policy file for *user1*, excluding flags set in the *userpolicy* file

```
The rsdpolicy file "user1" contains the following:
LOCKED=N
PASSWORD_CHANGE_REQUIRED=N
LOCK_REASON=
POLICY_FILENAME=userpolicy
PASSWORD_EXPIRATION=06/18/2003
WARNING_DAYS=10
MAX_CONSECUTIVE_LOGON_FAILURES=9
CONSECUTIVE_LOGON_FAILURES=0
This is the end of the rsdpolicy file
```

- ◆ List all RSD policy files that start with *user*:

```
ceupassrpt -r user*
```

In this example, the command displays the basic contents of the three files that begin with *user*:

```
The rsdpolicy file "user1" contains the following:
LOCKED=N
PASSWORD_CHANGE_REQUIRED=N
LOCK_REASON=
POLICY_FILENAME=userpolicy
PASSWORD_EXPIRATION=06/18/2003
WARNING_DAYS=10
MAX_CONSECUTIVE_LOGON_FAILURES=9
CONSECUTIVE_LOGON_FAILURES=0
This is the end of the rsdpolicy file
```

```
The rsdpolicy file "user2" contains the following:
LOCKED=N
PASSWORD_CHANGE_REQUIRED=N
LOCK_REASON=
POLICY_FILENAME=userpolicy
PASSWORD_EXPIRATION=06/18/2003
WARNING_DAYS=10
MAX_CONSECUTIVE_LOGON_FAILURES=9
CONSECUTIVE_LOGON_FAILURES=0
This is the end of the rsdpolicy file
```

```
The rsdpolicy file "user3" contains the following:
LOCKED=N
PASSWORD_CHANGE_REQUIRED=N
LOCK_REASON=
POLICY_FILENAME=userpolicy
PASSWORD_EXPIRATION=06/18/2003
WARNING_DAYS=10
MAX_CONSECUTIVE_LOGON_FAILURES=9
CONSECUTIVE_LOGON_FAILURES=0
This is the end of the rsdpolicy file
```

- ◆ List all RSD policy files that start with *user* and have passwords that expire on or before 03/31/2003:

```
ceupassrpt -r user* -e 03/31/2003
```

- ◆ List all RSD policy files that start with *user* and are governed by *policy1*:

```
ceupassrpt -r user* -p policy1
```

---

## Changing User Password

The **ceupasswd** utility enables users to change their current password in their RSD file.

---

**Note:** Use only the **ceupasswd** utility or the Sterling Connect:Enterprise for UNIX Site Administration user interface to change a password in an RSD file. Any other program invalidates the hash value.

---

The following table describes the **ceupasswd** command line parameters. Required parameters are in bold.

| Parameter                                    | Description                                                         | Value                                                                                         |
|----------------------------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| -H <i>hostname</i><br>--Host <i>hostname</i> | IP address or name of host where authentication service is running. | Host name or IP address where authentication service is running (optional if CMUHOST is set). |
| -P <i>portno</i><br>--Port                   | Port to connect to for authentication service.                      | Port number where authentication service is running (optional if CMUPORT is set).             |
| -u <b>userid</b><br>--userid                 | User ID of person executing <b>ceupasswd</b> .                      | Valid user ID. Required.                                                                      |
| -p <b>password</b><br>--password             | Password of person executing <b>ceupasswd</b> .                     | Current password. Required.                                                                   |
| -n <b>newpassword</b><br>--new               | New password.                                                       | New password. Required.                                                                       |
| -c <b>newpassword</b><br>--confirm           | Confirm new password.                                               | New password. Required.                                                                       |
| ?, -h<br>--help                              | Lists command line options (help).                                  | None.                                                                                         |

This example illustrates how *user1* changes his or her password from *mypass* to *newpass*:

```
ceupasswd -u user1 -p mypass -n newpass -c newpass
```

## Authentication Log File

The authentication log file (auth.log) records the following events:

- ◆ Changes to values in policy files, RSD policy files, and the password configuration file
- ◆ Verification or denial of access for a user by the authentication daemon

You can use a text editor to view the contents of this log file. The log file is stored in `$CMUHOME/log/auth.log`. Refer to *Authorization Log Message IDs* on page 253 for explanations about the error messages that display in this log file.



---

# Administrator Commands

Administrator commands are used specifically by the administrator to control the fundamental operations of Sterling Connect:Enterprise. The following special purpose utilities are supplied:

- ◆ Generate and administer the global key used for batch and password encryption (**ceukkey**)
- ◆ Generate the key used to encrypt internal product communications (**cmusipskey**)
- ◆ Generate key pairs for SSHFTP communications (**cmusshkey**)
- ◆ Encrypt existing passwords for RSD files (**ceupassencrypt**)
- ◆ Locate configuration problems before starting the repository (**cmucheckcfg**)
- ◆ Correct control file records to match repository batches present (**cmufixup**)
- ◆ Initialize a mailbox (**cmuinit**)
- ◆ Reconstruct repository database control files by scanning data batches (**cmurebuild**)
- ◆ Tracing Sterling Connect:Enterprise activity (**ceutrace**)

---

## Generating the Global Key (ceukkey)

Use the **ceukkey** command to generate the global keys necessary to encrypt both batches and RSD passwords. It creates `key.global` for strong and weak encryption and `deskey.global` for 3DES encryption.

---

**Caution:** Once activated, password encryption cannot be turned off. The global key files should not be deleted, moved, updated, or otherwise altered in any way after it has been used to encrypt a batch.

---

The following table describes the parameters available for **ceukkey**. All parameters may be input using either the single hyphen or double hyphen format. The parameters may be separated from their associated values by a space or the values may immediately follow.

| Parameter                                             | Description                                                                                 |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------|
| -c<br>--change                                        | Changes the passphrase                                                                      |
| -k <i>clearkey file</i><br>--key <i>clearkey file</i> | Specifies the full path of the existing clear key                                           |
| -t <i>cleardeskey file</i>                            | Specifies the full path of the existing clear 3DES key                                      |
| -p passphrase<br>--pass passphrase                    | Specifies the 6–32 character passphrase to encrypt the global key                           |
| -x<br>--encryptpass                                   | Turns on encryption for RSD passwords. Only valid when global key has already been created. |
| -?<br>--help                                          | Displays usage messages                                                                     |

For more specific instruction, Refer to one of the following.

- ◆ *Creating a Global Key* on page 128
- ◆ *Encrypting RSD Passwords* on page 129
- ◆ *Changing the Passphrase of the Global Key* on page 130.
- ◆ *Replacing Your Global Key* on page 130

## Creating a Global Key

Use the following procedure to create a global key and a 3DES global key for batch encryption:

1. Type the following command and press **Enter**:

```
ceukey
```

2. You are prompted with the following:

```
Please enter the passphrase (6--32 characters):
```

3. Type a passphrase to encrypt the global key and press **Enter**. You are prompted with the following:

```
Do you want PASSWORD encryption? [Y|n]
```

4. If you do not want to encrypt RSD passwords, type **n** and press **Enter**. You can encrypt RSD passwords at a later time. If you want to encrypt RSD passwords, type **y** and press **Enter**. You also need to run **ceupassencrypt**. Refer to *Encrypting Existing Passwords (ceupassencrypt)* on page 133.



You are prompted with the following:

```
Do you want to save clear keys into a file?[Y|n]
```

5. Saving the clear keys is a safety mechanism in case something happens to your global key.

To save in clear text, type **y** and press **Enter**. The clear key is saved as `$CMUHOME/keys/key.clear`. The clear key file contains a string of characters used to create the global key. Because the `$CMUHOME/keys` directory is not secure, it is up to you to save the clear key to a secure location.

You are prompted with the following:

```
Do you want to save des clear keys into a file?[Y|n]
```

6. Saving the des clear keys is a safety mechanism in case something happens to your 3DES global key.
7. Backup the `$CMUHOME/keys/key.global` and `$CMUHOME/keys/deskey.global` to an alternate location such as disk or hard copy to guard against the loss of encrypted data. The `$CMUHOME/keys` directory is not secure.
8. If you chose to save your keys in clear text in step 5 on page 129 and step 6 on page 129, move `$CMUHOME/keys/key.clear` and `$CMUHOME/keys/deskey.clear` to a secure location. The `$CMUHOME/keys` directory is not secure.
9. Restart Sterling Connect:Enterprise.

After you create the global key, batch encryption is allowed. However, you must activate each mailbox using the `encrypt.cfg` file. See the *IBM Sterling Connect:Enterprise for UNIX Configuration Files Reference Guide* for more information on the `encrypt.cfg` file

## Encrypting RSD Passwords

Before you can encrypt RSD passwords, you need to create a global key and 3DES global key. If you selected to encrypt RSD passwords when you created your global key and 3DES global key in *Creating a Global Key* on page 128, this procedure is not necessary. This procedure renames the current global key and creates a new global key.

1. Type the following command and press **Enter**:

```
ceukey -x
```

You are prompted with the following:

```
Please enter the passphrase:
```

2. Type the passphrase for the current global key and press **Enter**. You are prompted with the following:

```
Do you want to save clear keys into a file?[Y|n]
```

3. Saving the clear keys is a safety mechanism in case something happens to your global key.

To save in clear text, type **y** and press **Enter**. The clear key is saved as `$CMUHOME/keys/key.clear`. The clear key file contains a string of characters used to create the global key. Because the `$CMUHOME/keys` directory is not secure, it is up to you to save the clear key to a secure location.

You are prompted with the following:

```
The old key.global was renamed into /$CMUHOME/keys/key.global.20050418115918.
Do you want to keep it?[y|N]
```

4. To keep the existing global key, type **y** and press **Enter**.
5. Backup the `$CMUHOME/keys/key.global` to an alternate location such as disk or hard copy to guard against the loss of encrypted data. The `$CMUHOME/keys` directory is not secure.
6. If you chose to save your keys in clear text in step 3 on page 130, move `$CMUHOME/keys/key.clear` to a secure location. The `$CMUHOME/keys` directory is not secure.

## Changing the Passphrase of the Global Key

You can also use the **ceukey** command to change the passphrase of the global key. Use the following procedure:

1. Type the **ceukey** command as follows:

```
ceukey -c -p passphrase
```

where *passphrase* is the current passphrase for the global key.

You are prompted for a new passphrase.

2. Type the new passphrase and press **Enter**.  
You are prompted to confirm the new passphrase.
3. Type the new passphrase again and press **Enter**.

## Replacing Your Global Key

If something happens to your global key or 3DES global key, you cannot decrypt batches or RSD passwords. If you saved your encrypted global key to another location, you can copy it into `$CMUHOME/keys/key`. If you do not have a copy of the encrypted global key, but you have a copy of the clear key, use the following procedure to encrypt the global key using the clear key:

1. Copy the clear key and 3DES clear keys to an accessible directory.
2. Type the following command and press **Enter**:

```
ceukey -k pathtoclearkey -t pathtodesclearkey
```

where *pathtoclearkey* is the location of the clear key from step 1 on page 130 and *pathtodesclearkey* is the location of the 3DES clear key from step 1 on page 130.

You are prompted with the following:

```
Please enter the passphrase (6--32 characters):
```

3. Type a passphrase to encrypt the clear key and 3DES clear key.
4. Restart Sterling Connect:Enterprise.

---

## Creating SSH SFTP Keys (cmusshkey)

Use this command to create the SSH host key, or to create a key to associate with an account. The following table describes the valid parameters:

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -k                    | Specifies to generate a key. A host key is created unless you also specify the -r parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| -e                    | Specifies to export the key. Specify the path and file name of the key file to export using the -f parameter. Specify the path and file name of the export key file to create using the -F parameter.                                                                                                                                                                                                                                                                                                                                                                          |
| -i                    | Specifies to import a key file. Specify the path and file name of the import key file to create using the -f parameter. Specify the path and file name of the key file to import using the -F parameter.                                                                                                                                                                                                                                                                                                                                                                       |
| -l                    | Specifies to display the fingerprint of the public key.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -p                    | Specifies to change passphrase. You must also specify -N and -P.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| -r <i>accountname</i> | Specifies to create a key to associate with an account. The <i>accountname</i> is the name of the account (RSD) to create the key for. They key pair is stored as:<br>\$CMUHOME/ssh/users/sshftp/ <i>accountname</i> /id_rsa and<br>\$CMUHOME/ssh/users/sshftp/ <i>accountname</i> /id_rsa.pub.<br>You can specify a different name for the key using the -f parameter or when prompted.<br>If you do not specify this parameter, the public and private keys are stored in the current directory.<br>If you are changing the passphrase of a key, this parameter is required. |
| -f <i>path</i>        | Specifies the location to store the generated key. If you specify a directory and file name, the key is stored in the specified directory with the specified file name. If you only specify a directory, the key is stored in the specified directory and the file name defaults to id_rsa or id_dsa.                                                                                                                                                                                                                                                                          |
| -F <i>filename</i>    | Used with the -e parameter to specify the name of the file to export.<br>Used with the -i parameter to specifies the file to import.                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Parameter            | Description                                                                                                   |
|----------------------|---------------------------------------------------------------------------------------------------------------|
| -t <i>type</i>       | Specifies the type of key to create. Valid values are <b>rsa</b> and <b>dsa</b> . The default is <b>rsa</b> . |
| -b <i>nnnn</i>       | Specifies the key length in bytes. The default is 1024.                                                       |
| -N <i>passphrase</i> | Specifies the new passphrase. Used with -p.                                                                   |
| -P <i>passphrase</i> | Specifies the old passphrase. Used with -p.                                                                   |
| -v                   | Requests verbose display.                                                                                     |
| ?                    | Displays usage information.                                                                                   |

### Create a Host Key Pair

The following example creates a host key for the system. This is the command issued if you select to set up SSH during the installation:

```
cmusshkey -k
```

This command creates the public host key as `$CMUHOME/ssh/system/ssh_host_key.pub` and the private host key as: `$CMUHOME/ssh/system/ssh_host_key`.

### Create an RSD Key

The following example creates a key for the *user01* account:

```
cmusshkey -k -r user01 -f user01key -t rsa -b 2048
```

This command creates an rsa key pair that is 2048 bits in length. The public key is stored as: `$CMUHOME/ssh/users/sshftp/user01/user01key.pub`. The private key is stored as: `$CMUHOME/ssh/users/sshftp/user01/user01key`.

### Change the Passphrase on a Private Key

The following command changes the passphrase of the *user01key* private key from *oldpassphrase* to *newpassphrase*:

```
cmusshkey -p -f user01 -P oldpassphrase -N newpassphrase
```

---

## Encrypting Existing Passwords (ceupassencrypt)

When password encryption has been activated using **ceukey**, all passwords are encrypted for new RSD files. The **ceupassencrypt** command is used to encrypt passwords for RSD files that existed before password encryption was activated and to encrypt passwords for RSD files that were created using a text editor or were created by an automated script. The **ceupassencrypt** command should be used when upgrading from a previous version of Sterling Connect:Mailbox for UNIX or Sterling Connect:Enterprise for UNIX.

To encrypt existing RSD passwords, complete the following steps:

1. Select the appropriate parameters from the following table. You must use at least one parameter.

All parameters may be input using either the single hyphen or double hyphen format. The parameters may be separated from their associated values by a space or the values may immediately follow.

| Parameter                                                   | Description                                                  |
|-------------------------------------------------------------|--------------------------------------------------------------|
| -p <i>password</i><br>--password <i>password</i>            | Specifies the 1–8 character clear password for an RSD file   |
| -r <i>rsd file pattern</i><br>--rsd <i>rsd file pattern</i> | Specifies a set of RSD files for which to encrypt passwords. |
| -?<br>--help                                                | Displays usage messages                                      |

2. Enter the **ceupassencrypt** command similar to the following example, using the parameters and values determined in step 1. See *ceupassencrypt Example* on page 145 for additional examples using the **ceupassencrypt** command.

```
$> ceupassencrypt -r ""
```

This example encrypts passwords in all existing RSD files.

---

**Note:** Quotation marks are required to encrypt passwords in all existing RSD files.

---

## Locating Configuration Problems (cmucheckcfg)

The **cmucheckcfg** command checks configuration files for syntax errors and should be used to validate manually created or modified configuration files before use.

To locate configuration problems, complete the following steps:

1. Select the appropriate parameters from the following table. The required parameters are in bold.

All parameters must be input using the single hyphen format. The parameters may be separated from their associated values by a space or the values may immediately follow. Long parameters (those beginning with a double hyphen) are not supported for this command.

| Parameter                                                                                                         | Description                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>-t</b><br><b>{all acd rsd cpd med mcd spd acl enc}</b>                                                         | Type of configuration file<br>Note: The <i>enc</i> option specifies the <i>encrypt.cfg</i> file.                         |
| <b>-d</b> <i>debug_file</i>                                                                                       | Generates a debug file                                                                                                   |
| <b>-f</b> <i>cfg_filename</i>                                                                                     | Specifies a file to be checked                                                                                           |
| <b>-l</b> <i>debug_level</i>                                                                                      | Specifies debug level                                                                                                    |
| <b>-o</b> <i>output_filename</i>                                                                                  | Stores all results                                                                                                       |
| <b>-p</b> <i>{bsca}</i> - valid for AIX<br><b>-p</b> <i>{ftp bsc bscc async sshftp}</i> - valid for all platforms | Indicates CPD file protocol. The BSCC value is specific to Cleo SYNCcable+ connections.<br>(required for CPD files only) |
| <b>-v</b>                                                                                                         | Displays current values in configuration files                                                                           |

2. Enter the **cmucheckcfg** command similar to the following example, using the parameters and values determined in step 1. See *cmucheckcfg Example* on page 145 for additional examples using the **cmucheckcfg** command.

```
$> cmucheckcfg -tacd -fsteve.acd
```

## Correcting Control File Records (cmufixup)

The **cmufixup** program ensures that a mailbox's contents have not been corrupted. This utility validates that the *\$CMUHOME/med* file exists and that the entries in the control file match actual data batches in the repository. There are three modes to operating **cmufixup**.

- ◆ By default, **cmufixup** corrects any discrepancies in the database without prompting the user when they are found. If a mismatch is found, **cmufixup** deletes any mismatched batch and control record pairs that are found.

---

**Note:** If **cmufixup** finds any discrepancies in comparing the control records to the actual data files, an ASCII image of the original control records is stored in `$CMUHOME/database/BAD` as `batno.ctrl`, where `batno` is the original batch number for that control record.

---

- ◆ You can select interactive mode by specifying the **-i** parameter. This mode prompts the user to delete the mismatched batch and control record pairs.
- ◆ You can select diagnostic mode by specifying the **-n** parameter. This mode directs all responses from **cmufixup** to standard output. No mismatched batch and control record pairs are deleted.

The **cmufixup** program can search for and correct database discrepancies in nonencrypted and encrypted batches.

Use the following procedure to search for and correct discrepancies:

1. Select the appropriate parameters from the following table. All **cmufixup** parameters are optional; **-n** and **-i** are mutually exclusive.

All parameters must be input using the single hyphen format. The parameters may be separated from their associated values by a space or the values may immediately follow. Long parameters (those beginning with a double hyphen) are not supported for this command.

| Parameter          | Description                         |
|--------------------|-------------------------------------|
| <b>-C medfile</b>  | MED file name                       |
| <b>-c ctrldir</b>  | Path of control directory           |
| <b>-D</b>          | Generates a debug file              |
| <b>-d datadir</b>  | Path of data directory              |
| <b>-H hostname</b> | Host computer where cmuctld started |
| <b>-i</b>          | Prompts with interactive queries    |
| <b>-n</b>          | Specifies diagnostic only           |
| <b>-P portno</b>   | Port number where cmuctld started   |
| <b>-?</b>          | Displays usage messages             |

- ◆ Type the **cmufixup** command similar to the following example, using the parameters and values determined in step 1. See *cmufixup Examples* on page 146 for additional examples using the **cmufixup** command.

```
cmufixup -i
```

If the **cmufixup** program detects an encrypted batch, the following prompt is displayed after you issue the **cmufixup** command:

```
Detect encrypted batch(es)!
Please enter the global key's pass phrase:
```

- a. Type the passphrase you established when you created the global key (**ceukey**). Refer to *Generating the Global Key (ceukey)* on page 127 for more information about the global key.
- b. Press **Enter**.

The output of `cmufixup` lists problem batches to stdout in batch number sequence. If problems are found with a batch, a message lists the batch number and problem. The message describes the problem. Following is an example:

```
1000          Batch data file found but no control record in database
```

At the end of the run, a set of summary lines is produced. Following is an example:

```
Summary of Validation / Fix Up
Total Batches Seen           : 187
Maximum Batch Number        : 1000
Missing or extra index file  : 0
Missing or extra link file   : 0
Bad database control record  : 0
No data file                 : 0
No database control record   : 1
Bad header record in data file : 0
Invalid data file            : 0
Total records fixed          : 1
No action taken              : 186"
```

---

## Initializing a Mailbox (cmuinit)

The **cmuinit** program initializes a mailbox. It creates a mailbox and all of its associated control files. It also creates the Mailbox Engine Definitions file in the `$CMUHOME/med` directory. **cmuinit** must be executed on the computer where the mailbox is being created.

---

**Caution:** Perform **cmuinit** only on the advice of IBM Support.

---

To initialize a mailbox, complete the following steps:

1. Select the appropriate parameters from the following table. All parameters are optional.

All parameters must be input using the single hyphen format. The parameters may be separated from their associated values by a space or the values may immediately follow. Long parameters (those beginning with a double hyphen) are not supported for this command.



| Parameter         | Description                                  |
|-------------------|----------------------------------------------|
| -b <i>maxbno</i>  | Maximum batch number                         |
| -c <i>ctrldir</i> | Path of control directory                    |
| -d <i>datadir</i> | Path of data directory                       |
| -m <i>meddir</i>  | Path of directory for MED file               |
| -s <i>minfree</i> | Minimum free space                           |
| -p <i>prefix</i>  | Specifies prefix for Mailbox Engine database |
| -?                | Displays usage messages                      |

2. Enter the **cmuinit** command similar to the following example, using the parameters and values determined in step 1. See *cmuinit Example* on page 146 for additional examples using the **cmuinit** command.

```
cmuinit
```

This example initializes the mailbox and accepts all defaults.

---

## Reconstructing Repository Control Files (cmurebuild)

The **cmurebuild** utility validates the repository database and rebuilds the indices to improve performance and reclaim space (**cmurebuild -x**). It can also be used to completely rebuild the database, if it has been deleted or the data directory has been moved to a new location (**cmurebuild** without **-x**).

---

**Note:** In the following procedures, the specified paths assume the following parameters in the \$CMUHOME/med/cmumbox.med file, where \$CMUHOME is set to the Sterling Connect:Enterprise home directory:  
 ControlDir=\$CMUHOME/database  
 DataDir=\$CMUHOME/database/mailbox

The **cmurebuild -c** and **-d** parameters override the MED file values, if required.

---

### Reclaim Space and Improve Performance

Over time, as batches are added to the repository, the database index files grow large and become fragmented, affecting performance. You can run **cmurebuild -x** periodically to streamline the index files for performance and space. You should also run **cmurebuild -x** to correct database index corruption, which can be caused by a system crash during mailbox activity. The **cmurebuild -x**

command skips the full rebuild from repository data files. You can run it as long as there is an existing `cmumbox.dat` database file in the control directory. Complete the following steps:

1. Shut down Sterling Connect:Enterprise
2. Backup the `$CMUHOME/database/cmumbox*` files
3. Delete the `$CMUHOME/database/cmumbox*.idx` files (leaving `cmumbox.dat`)
4. Run `cmurebuild -x` to rebuild the index files. Optional argument `-c $CMUHOME/database`
5. Start Sterling Connect:Enterprise

## Rebuilding the Repository Database

If the data directory has been moved, the `cmumbox.dat` file is missing, or `cmurebuild -x` fails, you must run the full **cmurebuild**. In this case, the `cmurebuild` utility must have newly created and initialized database files in the control directory. It traverses the entire data directory and re-adds all of the valid batches to the new database. Corrupt and orphaned batches are deleted from the repository and relocated to `$CMUHOME/database/BAD/batno`, where `batno` is the batch number used as a file name. The **cmurebuild** utility then rebuilds the indices for performance. Complete the following:

1. Shut down Sterling Connect:Enterprise.
2. Backup `$CMUHOME/database` directory and all subdirectories beneath it. By default, the control directory is `$CMUHOME/database` and the data directory is `$CMUHOME/database/mailbox`. If your locations are different, backup the correct locations.
3. Delete all the `cmumbox*` database files from the control directory (for example, `$CMUHOME/database`):
  - ◆ `cmumbox.dat`
  - ◆ `cmumbox_bid.idx`
  - ◆ `cmumbox_bno.idx`
  - ◆ `cmumbox_rid.idx`
  - ◆ `cmumbox_tbib.idx`
  - ◆ `cmumbox_tridbid.idx`
4. Run `cmuinit` to create new, empty database files in the control directory.
5. Run `cmurebuild` with optional arguments `-c <control directory>` and `-d <data directory>`.
6. The `cmurebuild` utility re-adds all the batches found in the data, then falls through and rebuilds the indices for performance (the `cmurebuild -x`).
7. Start Sterling Connect:Enterprise.

---

## Tracing Sterling Connect:Enterprise Activity

You can use the dynamic tracing command (**ceutrace**) to turn tracing on and off and to set tracing levels without restarting Sterling Connect:Enterprise. You can also use **ceutrace** to view the current settings. Refer to the following procedures in this section:

- ◆ *Turning Tracing On* on page 139
- ◆ *Daemon Considerations* on page 143
- ◆ *Locating Your Trace Files* on page 144
- ◆ *Turning Tracing On* on page 139
- ◆ *Clearing and Restarting Your Trace Files* on page 144

### Turning Tracing On

Use the following procedure to turn tracing on:

1. Select the appropriate parameters from the following table. The required parameters are in bold.

All parameters may be input using either the single hyphen or double hyphen format. The parameters may be separated from their associated values by a space or the values may immediately follow.

| Parameter                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -o                                             | Turn trace on                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --on                                           | Turns tracing on at the target daemons and displays the current trace settings.<br>If --on is specified for a target daemon that is not actively tracing, a trace file is opened according to its current filename prefix.                                                                                                                                                                                                                                                                       |
| -x                                             | Turn trace off                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| --off                                          | Setting --on or --off will turn tracing on or off at the target daemon(s) and display the current trace settings. Setting neither causes the display of current settings. If --off is sent to a daemon that is actively tracing, it will turn off tracing and close its trace file. If --on is sent to a daemon that is not actively tracing, it will open a trace file according to its current filename prefix. --on and --off are mutually exclusive. If both are specified an error results. |
| -H <i>hostname</i><br>--host <i>hostname</i>   | Host computer where the control daemon was started.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| -P <i>portno</i><br>--port <i>portno</i>       | Port number where the control daemon was started.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| -p <i>password</i><br>--passwd <i>password</i> | Sterling Connect:Enterprise password                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Parameter                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d <i>daemon names</i><br>--daemon <i>daemon names</i> | Direct the command to those daemons that match the daemon name patterns. If not specified, the command applies to all daemons. The daemon name pattern string may be a combination of File Name Matching patterns, separated by commas. For example, if you have multiple FTP daemons you can trace for all FTP daemons by specifying:<br>ceutrace -d "FTP*" -on<br>Refer to <i>Daemon Considerations</i> on page 143.                                                                                                    |
| -m on off<br>--mailbox on off                          | Automatically starts mailbox tracing for calls that the specified protocol daemon initiates. This parameter is only available when used with protocol daemons.<br>This affects the mailbox daemon tracing state only when the mailbox daemon was previously not tracing, or was tracing at a lower trace level than the protocol daemon. It cannot cause the mailbox daemon to lower its trace level. The parameter takes an "on" or "off" value to indicate whether mailboxalso processing is to be enabled or disabled. |
| -f<br>--filename                                       | Trace filename prefix<br>Adjusts the file name prefix of the trace file. It overrides the -d filename if specified on the target daemon command line startup. If the target name differs from the current, the old file is closed, and the new one is opened. You can only use this parameter if there is only one target daemon for the command (for example, --daemon FTP).                                                                                                                                             |

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -l<br>--level     | <p>Specifies the trace level from 0 to 100 at which the target daemons trace. It overrides the -l level if specified on the target daemon command line startup. Setting a trace level does not imply turning traces on. They must be turned on with the -on parameter. The trace levels are as follows, with each higher number including all tracing for lower numbers.</p> <p>Note: Tracing will affect performance. Do not specify levels higher than 10 unless instructed by IBM.</p> <p>0 High level messages and errors only<br/> 1–2 Logon / Logoff activity, statistics<br/> 3–4 FTP command traffic, simple program logic flow<br/> 5–8 One-line inter-process Communication (SIPS) flow, more program flow<br/> 9 SIPS records dumped (first 176 bytes)<br/> 10–49 More exhaustive debugging<br/> 50–98 Full SIPS records dumped<br/> 99 All known debug output<br/> 100 Full SIPS records dumped (field by field)</p> <p>The Java daemons (cmuhttp, cmuediintd, and cmuadmind) have the following log4j logging levels:</p> <p>=0 off—No logging<br/> &lt;=5 sparse—Errors only<br/> &lt;=9 moderate—Errors and warnings only<br/> &lt;=50 detailed—Includes informational<br/> &lt;=99 verbose—Includes trace data</p> |
| -a<br>--account   | <p>Account names to trace. List multiple account names in a command separated list. You can also match file name patterns and you can use an exclamation (!) to exclude.</p> <p>For example, to trace the remotes RMT1, RMT2, ... RMT10, but not RMTTEST, turn on FTP tracing for all but RMTTEST by specifying:</p> <p>ceutrace -d FTP -on -account "RMT*,!RMTTEST"</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| -L<br>--listname  | <p>Autoconnect list names to trace. List multiple autoconnects in a command separated list. You can also match file name patterns and you can use an exclamation (!) to exclude.</p> <p>For example, a to trace the list names of LIST1.acd, LIST2.acd, ... LIST10.acd, but not LIST10.acd, turn on FTP tracing for just the LIST2.acd-LIST9.acd list names by specifying:</p> <p>ceutrace -d FTP -on -L "LIST*,!*10**"</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -D<br>--delimited | <p>Specifies to return pipe delimited output.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

2. Enter the **ceutrace** command similar to the following example, using the parameters and values determined in step 1 on page 139. See *cmuinit Example* on page 146 for additional examples using the **ceutrace** command.

```
ceutrace --on -d "FTP*" -l9
```

3. The status of each daemon is displayed. Following is an example:

| Command Line Parameters: |     |              |       |                 |
|--------------------------|-----|--------------|-------|-----------------|
| ceutrace                 |     |              |       |                 |
| Name                     | SID | Trace Status | Level | Filename Prefix |
| CONTROL                  | 1   | Off          | 0     | CONTROL.out     |
| SVD                      | 8   | Off          | 0     | SVD.out         |
| MAILBOX                  | 3   | Off          | 0     | MAILBOX.out     |
| EDIINT                   | 16  | Off          | 0     | cmuediintd.out  |
| ASYNCD                   | 14  | Off          | 0     | ASYNCD.out      |
| HTTP                     | 13  | Off          | 0     | cmuhttpd.out    |
| SSHFTP                   | 12  | Off          | 0     | SSHFTP.out      |
| FTP2                     | 11  | On           | 9     | FTP2.out        |
| FTP                      | 10  | On           | 9     | FTP.out         |
| ADMIN                    | 9   | Off          | 0     | cmuadmind.out   |
| EXITS                    | 5   | Off          | 0     | EXITS.out       |
| SYSLOG                   | 2   | Off          | 0     | SYSLOG.out      |
| ACD                      | 4   | Off          | 0     | ACD.out         |
| AUTH                     | 6   | Off          | 0     | AUTH.out        |

The following example shows the output with the **-D** option specified. The column correspond to the columns in standard output:

```
CONTROL|1|Off|0|CONTROL.out
SVD|8|Off|0|SVD.out
MAILBOX|3|Off|0|MAILBOX.out
EDIINT|16|Off|0|cmuediintd.out
ASYNCD|14|Off|0|ASYNCD.out
HTTP|13|Off|0|cmuhttpd.out
SSHFTP|12|Off|0|SSHFTP.out
FTP2|11|On|9|FTP2.out
FTP|10|On|9|FTP.out
ADMIN|9|Off|0|cmuadmind.out
EXITS|5|Off|0|EXITS.out
SYSLOG|2|Off|0|SYSLOG.out
ACD|4|Off|0|ACD.out
AUTH|6|Off|0|AUTH.out
```

The trace output is written to one or more files. Refer to *Locating Your Trace Files* on page 144.

## Daemon Considerations

When specifying daemons to trace on, you must indicate the name of the daemon with the `-d` option. Following is a list of default daemon names. If these defaults have changed, you can look at the startup script for current values:

| Daemon  | Default Name                      |
|---------|-----------------------------------|
| CONTROL | cmuctld, mailbox control server   |
| AUTH    | cmuauthd, authentication server   |
| SVD     | cmusvid, service interface server |
| MAILBOX | cmumboxd, mailbox server          |
| ASYNCD  | cmuasyd, async daemon             |
| BISYNC  | cmubscdc, bisync daemon           |
| EDIINT  | cmuediintd, ediint daemon         |
| HTTP    | cmuhttpd, http daemon             |
| SSHFTP  | cmusshftpd, ssh daemon            |
| FTP     | cmuftpd, ftp daemon               |
| ADMIN   | cmuadmin, admin daemon            |
| EXITS   | cmuexitd, exits server            |
| SYSLOG  | cmulogd, log server               |
| ACD     | cmuacd, autoconnect server        |

With `ceutrace`, each daemon is managed differently by Sterling Connect:Enterprise. Consider the following when tracing the activity of a daemon.

- ◆ Business processes—The `ceutrace` command does not work with the business process daemon. The trace must be set at startup using `ceustartup.trace`.
- ◆ The `ceutrace` command does not affect the tracing status of child processes for the control daemon, authentication server daemon, mailbox daemon, log daemon, exit daemon, service interface daemon, FTP daemon, SSH daemon.
- ◆ The `ceutrace` command affects the tracing status of child processes of the autoconnect daemon.
- ◆ The `cmusvid` children created to serve a particular GUI user session are active for the life of that session and are not affected by the trace status changes during their lifetimes.
- ◆ Async and bisync remote connect child processes run continuously on a given port and do not end after each Remote Connect session. They when an autoconnect request is run on the same port. Any changes to tracing status specified using the `ceutrace` command for the master async or bisync daemon only take effect for the child processes on a given port when an autoconnect request is run on that port.
- ◆ Async and bisync remote connect sessions now have unique session IDs.

## Locating Your Trace Files

Sterling Connect:Enterprise creates a trace file for each daemon. The name of the files are generated as follows for all master daemons: `<prefix>.<pid>`, where `<prefix>` is the trace filename prefix specified on the command line for the master daemon using the `-d` parameter and `<pid>` is the process ID assigned to the daemon by the operating system.

The name of the trace files for slave and child processes is generated as follows:

| Master Daemon                      | Child or Slave Daemon Trace File Name                                                                                                                                                                                                                                                    |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Connect Daemon (cmuacd)       | <code>&lt;prefix&gt;.SLV.&lt;pid&gt;</code>                                                                                                                                                                                                                                              |
| Async Daemon (cmuasyd)             | Trace files for remote connect sessions are initially created as:<br><code>&lt;prefix&gt;.&lt;port-name&gt;.&lt;pid&gt;</code> .<br>Once a session is established the file is renamed to<br><code>&lt;prefix&gt;.&lt;port-name&gt;.&lt;account&gt;.&lt;session-ID&gt;.&lt;pid&gt;</code> |
| FTP Daemon (cmuftpd)               | For remote connections:<br><code>&lt;prefix&gt;.svr.&lt;account&gt;.&lt;sessionID&gt;.&lt;pid&gt;</code><br>For autoconnects:<br><code>&lt;prefix&gt;.clt.&lt;account&gt;.&lt;sessionID&gt;.&lt;pid&gt;</code>                                                                           |
| SSH Daemon (cmusshftp)             | <code>&lt;prefix&gt;.&lt;direction&gt;.&lt;function&gt;.&lt;account&gt;.&lt;sessionID&gt;.&lt;pid&gt;</code>                                                                                                                                                                             |
| Bisync Daemon (cmubscda, cmubscdc) | Trace files for remote connect sessions are initially created as:<br><code>&lt;prefix&gt;.&lt;port-name&gt;.&lt;pid&gt;</code> .<br>Once a session is established the file is renamed to<br><code>&lt;prefix&gt;.&lt;port-name&gt;.&lt;account&gt;.&lt;session-ID&gt;.&lt;pid&gt;</code> |

## Clearing and Restarting Your Trace Files

To manage the size of your trace files, you will need to periodically start new trace files. You have two options:

- ◆ If you want to save old trace files, you can rename the files in the trace directory and reissue the trace command using *Turning Tracing On* on page 139.
- ◆ If you do not want to save old trace files, reissue the trace command using *Turning Tracing On* on page 139.



---

## Examples

This section provides examples of some Administrator commands.

### ceukey Example

To replace a corrupted or missing global key file, use the **-k** parameter as in the following example:

```
ceukey -k $CMUHOME/keys/key.clear
```

### ceupassencrypt Example

To create an encrypted password for an RSD file created using a script, use the **-p** parameter as in the following example:

```
ceupassencrypt -p mypwd
```

---

**Note:** *mypwd* is the clear password.

---

The system responds with the encrypted version of the clear password.

```
ENCRYPTED_yzPJI/:ABJo3y
```

### cmucheckcfg Example

This example uses an ACD file called *steve.acd*. Note that it has one error in it. The *mbxsep* parameter is defined as *unknown\_junk*, which the parser does not recognize.

```
CONTACT = DATA_IMMEDIATE
ACPRRIORITYLEVEL = 07
RETRIES = 0
sessions=1
REQUEUES = 0
Interval = 0

REMOTE = "steve"
  ADDRESS ="hp816"
  MODE = SENDONLY
  sunique=yes
  mbxsep=unknown_junk
  bchsep=opt4
  ren_file=N
  acsenddir=/users/george/temp
  remotefilename="lll_yyy"
  sendid=george1,george
```

Type the following command:

```
$> cmucheckcfg -tacd -fsteve.acd
```

Here is the output:

```
====> Checking ACD file: /home/george/cmunix/acd/steve.acd...
        ERROR: Unrecognized "unknown_junk" on line 10 in ACD=steve.acd
<==== Completed checking ACD file: /home/george/cmunix/acd/steve.acd.
```

The **cmucheckcfg** command detected the error on line 10.

## cmufixup Examples

To check the integrity of the current repository contents, assuming that the repository directory and the control file prefixes are default values and interactive mode is desired, input the following:

```
cmufixup -i
```

## cmurebuild Example

To reclaim space and improve performance:

```
cmurebuild -x
Date: 03/04/11          IBM Sterling Connect:Enterprise for UNIX 2.5.00 Build 44
Time: 11:05:54          Validate Mailbox Database, Rebuild Indices
                        Target control (database) directory:
                        /data/CEU/ahmi_ce2500/database
Time: 11:05:54          Now validating database and rebuilding index files.
Time: 11:05:55          Index rebuild is complete. Now sorting delete chain.
Time: 11:05:55          1251 active records in database. Highest batch number: 1251
Time: 11:05:55          Processing complete for cmurebuild.
```

## cmuinit Example

To initialize the mailbox and override the minimum free space requirement, enter the following command:

```
cmuinit -s 1000000
```

## cmrebuild Example

To rebuild the repository database:

```
$ cmurebuild
Date: 01/27/04      IBM Sterling Connect:Enterprise for UNIX
Time: 14:53:05      Rebuild Mailbox Database

    Rebuilding from Mailbox directory: /ceunix/database/mailbox
    Into Database files located in   : /ceunix/database

    Batches added so far:      1000

Time: 14:53:18 Mailbox database rebuild is complete.
                Total Batches Seen: 1530
                Batches Added:      1529
                Batches bypassed:   4

                Deleting 8 database records used for padding.
                Moving 4 bypassed files to /ceunix/database/BAD

Time: 14:53:18 Now validating database and rebuilding index files.

Time: 14:53:18 Index rebuild is complete. Getting record counts.

Time: 14:53:18 1529 active records in database. Highest batch number: 1537

Time: 14:53:18 Processing complete for cmurebuild
```



---

## Generating Reports

Reports are generated using the **cmureport** utility. These reports provide the following information:

- ◆ **Auto Connect reports** follow the operation of all auto connect sessions.
- ◆ **Queued Auto Connect reports** show a history of all queued auto connects.
- ◆ **Remote Connect reports** summarize all sessions initiated by remote sites to the host.
- ◆ **Offline Utility Log reports** show all local user command line utility activity.
- ◆ **AS2 reports** follow the activity of all AS2 contracts.

---

### cmureport Utility

Reports are generated by using the **cmureport** utility.

Required parameters are in bold in the following table. All parameters (required or optional) can be input using either the abbreviated or long format.

The abbreviated parameters, those beginning with a single hyphen, may be separated from their associated values by a space or the values may immediately follow, without separation.

For specific information about each parameter and the associated values, see the page referenced in the right-hand column.

| Parameter                                                                                  | Description                                |
|--------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>-s rcs rcd acs acd acq off</b><br><b>--type rcs rcd acs acd acq off</b>                 | <b>Specifies Report type.</b>              |
| -?<br>--help                                                                               | Lists command line options (help).         |
| -B [CC]yyymmdd nnn[:hhmm]/hhmm][[:hhmm]<br>--Begin<br>[CC]yyymmdd nnn[:hhmm]/hhmm][[:hhmm] | Selects batches created on or before date. |

| Parameter                                                                           | Description                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -c<br>--csv, comma-separated output (option r only)                                 | Generates comma-separated report output based on selection type so output can be reformatted easily by another application. Valid only with -r option.                                                                                                                                           |
| -d<br>--delimit, pipe delimited ( )                                                 | Generates log data report output in pipe-delimited format. If a delimited report is run, then the failed adds show up with non-zero status codes.                                                                                                                                                |
| -f [CC]yyymmdd nnn[:hhmm/hhmm][hhmm]<br>--from<br>[CC]yyymmdd nnn[:hhmm/hhmm][hhmm] | Selects batches created on or after date.                                                                                                                                                                                                                                                        |
| -F log filename<br>--name log filename                                              | Specifies name of log file.                                                                                                                                                                                                                                                                      |
| -i remotename<br>--rmt remotename                                                   | Specifies that -srcd or -srcs is required.                                                                                                                                                                                                                                                       |
| -L listname<br>--list listname                                                      | Specifies auto connect (schedule) list name.                                                                                                                                                                                                                                                     |
| -M<br>--more                                                                        | Posts output messages one screen at a time.                                                                                                                                                                                                                                                      |
| -N number<br>--files number                                                         | Specifies number of log files to use.                                                                                                                                                                                                                                                            |
| -p pathname<br>--path pathname                                                      | Specifies location of logacct.dat files.                                                                                                                                                                                                                                                         |
| -r<br>--report, pipe-delimited ( ) output                                           | Generates normal cmureport output in pipe-delimited format. This option is intended to produce output that can easily be imported into applications accepting a pipe-delimited or comma-separated format. This option applies to all cmureport options (-srcd, -srcs, sacd, -sacq, -sacs, -soff) |
| -S f s a<br>--status f s a                                                          | Returns the status.                                                                                                                                                                                                                                                                              |
| -t [CC]yyymmdd nnn[:hhmm/hhmm][hhmm]<br>--to [CC]yyymmdd nnn[:hhmm/hhmm][hhmm]      | Selects batches created on or before date.                                                                                                                                                                                                                                                       |
| -T [CC]yyymmdd nnn[:hhmm/hhmm][hhmm]<br>--TO<br>[CC]yyymmdd nnn[:hhmm/hhmm][hhmm]   | Selects batches ending on or before date.                                                                                                                                                                                                                                                        |
| -v<br>--verbose                                                                     | Displays session activity.                                                                                                                                                                                                                                                                       |
| -X nnnn<br>--cols nnnn                                                              | Specifies columns available for screen display.                                                                                                                                                                                                                                                  |
| -Y nnnn<br>--rows nnnn                                                              | Specifies rows available for screen display.                                                                                                                                                                                                                                                     |

## Generating Reports

The following command generates an autoconnect (schedule) detail report in comma-separated format:

```
cmureport -sacd -r -c
```

The output of the comma-separated autoconnect (schedule) detail report command is as follows:

```
qatesthp,qatest,2003/01/10 09:08:26,2003/01/10 9:08:26,0,2,READ2,,622,1,
```

The following command generates a comma-separated, detail report for a remote account connection:

```
cmureport -srcd --report --csv
```

The output of the comma-separated, remote detail report command is as follows:

```
qatest,2003/01/10 09:08:26,2003/01/10 09:08:26,4128,3,,,0,0,
qatest,2003/01/10 09:08:26,2003/01/10 09:08:26,4128,3,,,0,0,
qatest,2003/01/10 09:08:26,2003/01/10 09:08:27,0,1,qatest,qatest,622,4,
qatest,2003/01/10 09:08:27,2003/01/10 09:08:27,4128,3,,,0,0,
qatest,2003/01/10 09:08:27,2003/01/10 09:08:27,4128,3,,,0,0,
```

The following command generates a pipe-delimited autoconnect (schedule) detail report:

```
cmureport -r -sacd
```

The output of the pipe-delimited autoconnect (schedule) detail report command is as follows:

```
serv01hp|serv01|2003/01/10 09:08:26|2003/01/10 09:08:26|0|2|READ2||622|1|
```

## Displaying and Printing Reports

After they are generated, reports can be redirected to a file or piped to the printer process for printing. This is done by redirecting the output to a specific file name using the greater than (>) symbol or piping to the printer with the | symbol.

To display the report, output the report to a file name as shown in the following example.

```
cmureport -s acd -L listname -p pathname > report1
```

Use a text editor to open the specified report name and review the results.

To print the report, pipe to the printer process as shown in the following example:

```
cmureport -S acd -L listname -p pathname | lp
```

If an error is encountered during parsing of the command line, error messages are written to standard error.

### Displaying Pipe-Delimited Reports

In addition to standard report formats, you can use the cmureport utility to produce all session details into a pipe-delimited output. You can create custom reports by parsing this output. The following command produces all session details in a pipe-delimited format:

**Note:** When the -d parameter is used with cmureport, some cmuadd offline utility failures are also shown in the report.

```
cmureport -d -v
```

The output of this command is 25 pipe-delimited fields. Following is an example:

```
0|40|434d5532|user01|2004/03/18 13:04:24|10|4|2004/03/18  
13:04:24|0|0|0|545|545|1|0|0|0|0|0|0|user01|test.file|||  
0|40|434d5532|user01|2004/03/18 13:04:31|11|4|2004/03/18  
13:04:31|0|0|0|545|545|1|2|0|0|0|0|0|user01|test.file|||  
0|10|434d5532|user01|2004/03/18 13:04:49|13|1|1969/12/31  
18:00:00|0|0|0|3|0|0|0|0|0|0|0|0|0|0|0|0|||
```

Not all fields apply for each record type. If a field does not apply it is blank or zero. The following table, organized by record type, indicates what fields apply to each record type:

| Record Type                | Applicable Fields                                             |
|----------------------------|---------------------------------------------------------------|
| Remote session start       | 1, 2, 3, 4, 5, 6, 7, 12                                       |
| Remote session information | 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 16, 17, 22, 23    |
| Remote session end         | 1, 2, 3, 4, 5, 6, 7, 8, 10, 16, 17, 18, 19, 20                |
| Auto connect session start | 1, 2, 3, 4, 5, 6, 7, 23                                       |
| Auto connect remote start  | 1, 2, 3, 4, 5, 6, 7, 12, 22                                   |
| Auto connect information   | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14, 15, 16, 17, 22, 23, 24 |
| Auto connect remote end    | 1, 2, 3, 4, 6, 7, 8, 9, 22                                    |
| Auto connect session end   | 1, 2, 3, 4, 6, 7, 8, 10, 16, 17, 18, 19, 23                   |
| Queued auto connect        | 1, 2, 3, 4, 5, 6, 7, 10, 11, 23                               |



| Record Type     | Applicable Fields                                      |
|-----------------|--------------------------------------------------------|
| Offline command | 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 16, 22, 23 |

The following table, organized by field position, describes each field and indicates which record type each field is valid for:

| Field Position | Valid for Records                                                                                                                                                                                         | Description                                                                                                                                                                                                                |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1              | All                                                                                                                                                                                                       | Delete flag. This value is zero for all record types.                                                                                                                                                                      |
| 2              | All                                                                                                                                                                                                       | Identifies the type of record.<br>10 = Remote connect records<br>20 = Auto connect records<br>30 = Queued auto connect records<br>40 = Offline utilities                                                                   |
| 3              | All                                                                                                                                                                                                       | Version. This value is CMU2 in hexadecimal notation for all record types.                                                                                                                                                  |
| 4              | All                                                                                                                                                                                                       | Remote name for remote connections, auto connect list name for auto connects and queued auto connects, or user name for offline utilities.                                                                                 |
| 5              | Remote session start<br>Remote session information<br>Remote session end<br>Auto connect session start<br>Auto connect remote start<br>Auto connect information<br>Queued auto connect<br>Offline command | Start date and time.                                                                                                                                                                                                       |
| 6              | All                                                                                                                                                                                                       | Sterling Connect:Enterprise session number. Valid for all record types.                                                                                                                                                    |
| 7              | All                                                                                                                                                                                                       | Message type. Indicates the type of information in the record:<br>1 = Remote connect start<br>2 = Auto connect remote start<br>3 = Remote information<br>4 = Offline information<br>5 = Remote end<br>6 = Auto connect end |

| Field Position | Valid for Records                                                                                                                                      | Description                                                                                                                                                                                                                         |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8              | Remote session information<br>Remote session end<br>Auto connect information<br>Auto connect remote end<br>Auto connect session end<br>Offline command | End date and time.                                                                                                                                                                                                                  |
| 9              | Auto connect information<br>Auto connect remote end                                                                                                    | Sub message type. For auto connect information, this is the remote function code:<br>1 = Add<br>2 = Request<br>3 = Directory<br>4 = Delete<br>5 = NOOP<br><br>For auto connect remote end records, this is the auto connect status. |
| 10             | Remote session information<br>Remote session end<br>Auto connect information<br>Auto connect session end<br>Queued auto connect<br>Offline command     | Status code for the remote command. Values are noted in <i>Appendix A, Error Messages</i> , in the <i>IBM Sterling Connect:Enterprise for UNIX Installation and Administration Guide</i> .                                          |
| 11             | Remote session information<br>Queued auto connect                                                                                                      | Function code:<br>1 = Add<br>2 = Request<br>3 = Directory<br>4 = Delete<br>5 = NOOP                                                                                                                                                 |
| 12             | Remote session start<br>Auto connect remote start                                                                                                      | Protocol<br>1 = TCP/IP (offline)<br>2 = Async<br>3 = FTP<br>4 = BSC<br>5 = Secure FTP                                                                                                                                               |
| 13             | Remote session information<br>Auto connect information<br>Offline command                                                                              | Batch size in bytes of the batch affected by the command. Accurately reports batch sizes less than 2,147,483,647 bytes. Batch sizes larger than 2,147,483,647 bytes are reported as zero.                                           |

| <b>Field Position</b> | <b>Valid for Records</b>                                                                                                          | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14                    | Remote session information<br>Auto connect information<br>Offline command                                                         | Size in bytes of the batch affected by the command. Valid for Accurately reports all file sizes.                                                                                                                                                                                                                                                                                                                   |
| 15                    | Remote session information<br>Auto connect information<br>Offline command                                                         | Batch number assigned by Sterling Connect:Enterprise.                                                                                                                                                                                                                                                                                                                                                              |
| 16                    | Remote session information<br>Remote session end<br>Auto connect information<br>Auto connect session end<br>Offline command       | This parameter has different meanings for different record types as follows:<br>For remote session end, this is the number of batches added during the session.<br>For auto connect session end, this is the number of batches added (received).<br>For offline commands, this is the offline function code:<br>0 = Add<br>1 = Extract<br>2 = Status<br>3 = Deleted<br>4 = Erase                                   |
| 17                    | Remote session information<br>Remote session end<br>Auto connect information<br>Auto connect session end                          | For remote session end, this is the number of batches requested during the session.<br>For auto connect session end, this is the number of batches requested.                                                                                                                                                                                                                                                      |
| 18                    | Remote session end                                                                                                                | For remote session end, this is the number of directory requests.                                                                                                                                                                                                                                                                                                                                                  |
| 19                    | Remote session end<br>Auto connect session end                                                                                    | The number of batches deleted                                                                                                                                                                                                                                                                                                                                                                                      |
| 20                    | Remote session end<br>Auto connect session end                                                                                    | The number of batches added without \$\$ADD.                                                                                                                                                                                                                                                                                                                                                                       |
| 21                    | For future use                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 22                    | Remote session information<br>Auto connect remote start<br>Auto connect information<br>Auto connect remote end<br>Offline command | For remote session information, auto connect information, and offline command, this is the mailbox ID affected by the command that was issued by the remote user. It may or may not correspond to an RSD.<br>For auto connect remote start and auto connect end, this is the mailbox ID specified in the remote block used in the current phase of the autoconnect attempt. This mailbox ID corresponds to an RSD. |

| Field Position | Valid for Records                                                                                                                                          | Description                                                                                                                                                                                                                                                                                                                                                         |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23             | Remote session information<br>Auto connect session start<br>Auto connect information<br>Auto connect session end<br>Queued auto connect<br>Offline command | For remote session information and auto connect information, this is the batch ID assigned by Sterling Connect:Enterprise.                                                                                                                                                                                                                                          |
| 24             | Auto connect information                                                                                                                                   | Name of the remote, this is the mailbox ID specified in the remote block used in the current phase of the autoconnect attempt. This mailbox ID corresponds to an RSD.                                                                                                                                                                                               |
| 25             | Remote session information<br>Auto connect remote start<br>Auto connect information                                                                        | For the business process (BP) protocol, this is the Sterling B2B Integrator workflow ID and the Sterling B2B Integrator status URL.<br><br>For the Autoconnect remote start records, this is the daemon name that processed the connection. If the protocol is async or bisync the daemon name is followed by the device name. For example:<br><br>BISYNC:/dev/ttya |

## Auto Connect Detail Report

The Auto Connect Detail Report lists details about each batch of data sent or received for each remote site that meet the criteria specified on the command line.

For each autoconnect (schedule) detail report, the following information is reported:

| Date: mm/dd/yy           | IBM Sterling Connect:Enterprise for UNIX |                   |          |          |      |     | Page: 0001 |      |
|--------------------------|------------------------------------------|-------------------|----------|----------|------|-----|------------|------|
| Time: hh:mm:ss           | Report Utility                           |                   |          |          |      |     |            |      |
| Command Line Parameters: |                                          |                   |          |          |      |     |            |      |
| cmureport                |                                          |                   |          |          |      |     |            |      |
| -sacd                    |                                          |                   |          |          |      |     |            |      |
| ListName                 | Remote                                   | Start             | End      | Id       | Bno  | T/C | Status     | BpId |
| xxxxxxxx                 | xxxxxxxx                                 | yy/mm/dd-hh:mm:ss | hh:mm:ss | xxxxxxxx | nnnn | x   | nnn        | nnnn |
| xxxxxxxx                 | xxxxxxxx                                 | yy/mm/dd-hh:mm:ss | hh:mm:ss | xxxxxxxx | nnnn | x   | nnn        | nnnn |
| xxxxxxxx                 | xxxxxxxx                                 | yy/mm/dd-hh:mm:ss | hh:mm:ss | xxxxxxxx | nnnn | x   | nnn        | nnnn |
| xxxxxxxx                 | xxxxxxxx                                 | yy/mm/dd-hh:mm:ss | hh:mm:ss | xxxxxxxx | nnnn | x   | nnn        | nnnn |
| xxxxxxxx                 | xxxxxxxx                                 | yy/mm/dd-hh:mm:ss | hh:mm:ss | xxxxxxxx | nnnn | x   | nnn        | nnnn |

The following table explains the columns:

| Column   | Description                                                                                                                                                                                                                                                                                                                             |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ListName | The name listed in the ACD file for this session. If the ACD file name is longer than 8 characters, only the first 8 will be displayed.                                                                                                                                                                                                 |
| Remote   | The remote site ID for the remote site contacted. If alternate routing is used, this field shows the actual RSD name that completed the transfer of data. For example, ABC@1 is shown rather than ABC. If the account that added the batch is a Sterling B2B Integrator account, this column shows the Sterling B2B Integrator user ID. |
| Start    | The date and time the remote site was contacted.                                                                                                                                                                                                                                                                                        |
| End      | The time processing was completed for the remote site.                                                                                                                                                                                                                                                                                  |
| ID       | 1–8 character ID. This is the mailbox ID of the batch.                                                                                                                                                                                                                                                                                  |
| Bno      | The 1–10 digit internal batch number assigned to the batch.                                                                                                                                                                                                                                                                             |
| T/C      | A single character code that indicates if the batch was collected (C), transmitted (T), or the batch had an error during collection/transmission (?).                                                                                                                                                                                   |
| Status   | A 4-digit failure code that identifies the processing status of the entire auto connect list. Convert Auto Connect Failure Codes from decimal to hexadecimal and search for a description in Appendix A, <i>Error Messages</i> .                                                                                                        |
| BpId     | Specifies the business process ID associated with the event.                                                                                                                                                                                                                                                                            |

## Auto Connect Summary Report

The Auto Connect Summary Report lists the auto connect records that matched the criteria specified on the command line. For each auto connect record, the following information is reported:

|                          |                                          |          |       |       |       |           |        |
|--------------------------|------------------------------------------|----------|-------|-------|-------|-----------|--------|
| Date: mm/dd/yy           | IBM Sterling Connect:Enterprise for UNIX |          |       |       |       | Page 0001 |        |
| Time: hh:mm:ss           | Report Utility                           |          |       |       |       |           |        |
| Command Line Parameters: |                                          |          |       |       |       |           |        |
| cmureport                |                                          |          |       |       |       |           |        |
| -sacs                    |                                          |          |       |       |       |           |        |
| List                     | Start                                    | End      | SXmt  | Scol  | FXmt  | FCol      | Status |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnnnn | nnnnn | nnnnn | nnnnn     | nnn    |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnnnn | nnnnn | nnnnn | nnnnn     | nnn    |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnnnn | nnnnn | nnnnn | nnnnn     | nnn    |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnnnn | nnnnn | nnnnn | nnnnn     | nnn    |

The following table explains the columns:

| Column | Description                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| List   | The name listed in the ACD file for this session. If the ACD file name is longer than 8 characters, only the first 8 characters will be displayed.                                                                                  |
| Start  | The date and time the auto connect started processing.                                                                                                                                                                              |
| End    | The time the auto connect completed processing.                                                                                                                                                                                     |
| SXmt   | The number of the successful batch transmissions to the remote sites on the auto connect list.                                                                                                                                      |
| Scol   | The number of successful batch transmissions collected from the remote sites on the auto connect list.                                                                                                                              |
| FXmt   | The number of unsuccessful batch transmissions to the remote sites on the auto connect list.                                                                                                                                        |
| FCol   | The number of unsuccessful batch collections from the remote sites on the auto connect list.                                                                                                                                        |
| Status | A 4-digit failure code that identifies the processing status of the entire auto connect list.<br>Convert Auto Connect Failure Codes from decimal to hexadecimal and search for a description in Appendix A, <i>Error Messages</i> . |

## Remote Connect Detail Report

The Remote Connect Detail Report lists details about each communications session with a remote site. The report identifies when a remote site connected/disconnected with Sterling Connect:Enterprise and when each remote site command was processed by Sterling Connect:Enterprise.

| Date: mm/dd/yy           | IBM Sterling Connect:Enterprise for UNIX |          |        |         |         | Page: 0001 |       |
|--------------------------|------------------------------------------|----------|--------|---------|---------|------------|-------|
| Time: hh:mm:ss           | Report Utility                           |          |        |         |         |            |       |
| Command Line Parameters: |                                          |          |        |         |         |            |       |
| cmureport                |                                          |          |        |         |         |            |       |
| -srcd                    |                                          |          |        |         |         |            |       |
| Remote                   | Start                                    | End      | Status | Func ID | Bno     | Count      | BpId  |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnn    | xxx     | nnnnnnn | nnnnn      | nnnnn |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnn    | xxx     | nnnnnnn | nnnnn      | nnnnn |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss | nnn    | xxx     | nnnnnnn | nnnnn      | nnnnn |

Each Remote Connect Detail Report contains the following information:

| Column | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote | The name of the remote site that connected to Sterling Connect:Enterprise.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Start  | The date and time processing started for the event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| End    | The time that processing was completed for the event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Status | A 4-digit failure code associated with a failed remote connect. Remote Connect Failure Codes are documented in Appendix A, <i>Error Messages</i> .                                                                                                                                                                                                                                                                                                                                                                                  |
| Func   | The 3- or 4-byte field that describes the event being reported. Function types are:<br>CON-The remote site connected to Sterling Connect:Enterprise.<br>DISC-The remote site disconnected from Sterling Connect:Enterprise.<br>ADD-The remote site sent an \$\$ADD or put command.<br>REQ-The remote site sent a \$\$REQUEST or get command.<br>DEL-The remote site sent a \$\$DELETE or del command.<br>DIR-The remote site sent a \$\$DIRECTORY or dir command.<br>NOP- An event occurred while trying to establish a connection. |
| ID     | The 1–8 character mailbox ID of the batch(s).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Bno    | The internal 8-digit batch number assigned to the batch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Count  | The number of batch bytes transmitted/received (protocol overhead is not included in this count).                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Column | Description                                                  |
|--------|--------------------------------------------------------------|
| Bpld   | Specifies the business process ID associated with the event. |

## Remote Connect Summary Report

The Remote Connect Summary Report lists the remote connect summary records that match the criteria specified on the command line.

|                          |                                          |            |      |      |      |      |      |
|--------------------------|------------------------------------------|------------|------|------|------|------|------|
| Date: mm/dd/yy           | IBM Sterling Connect:Enterprise for UNIX | Page: 0001 |      |      |      |      |      |
| Time: hh:mm:ss           | Report Utility                           |            |      |      |      |      |      |
| Command Line Parameters: |                                          |            |      |      |      |      |      |
| cmureport                |                                          |            |      |      |      |      |      |
| -srcs                    |                                          |            |      |      |      |      |      |
| Remote                   | Start                                    | End        | Add  | woA  | Req  | Dir  | Del  |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss   | nnnn | nnnn | nnnn | nnnn | nnnn |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss   | nnnn | nnnn | nnnn | nnnn | nnnn |

The following table explains the columns:

| Column | Description                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------|
| Remote | The name of the remote site that connected to Sterling Connect:Enterprise.                                                     |
| Start  | The date and time the remote site connected to Sterling Connect:Enterprise.                                                    |
| End    | The time that processing was completed for the remote site.                                                                    |
| Add    | The number of batches of data that were successfully added by the remote site using the <b>\$\$ADD</b> or <b>put</b> commands. |
| woA    | The number of batches of data that were successfully added <i>without</i> using the <b>\$\$ADD</b> or <b>put</b> command.      |
| Req    | The number of batches that were transmitted in response to <b>\$\$REQUEST</b> or <b>get</b> commands.                          |
| Dir    | The number of <b>\$\$DIRECTORY</b> or <b>dir</b> commands issued by the remote site.                                           |
| Del    | The number of successfully-processed <b>\$\$DELETE</b> or <b>del</b> commands issued by the remote site.                       |



## Queued Auto Connect Report

The Queued Auto Connect Report lists the auto connect records that match the criteria specified on the command line. The records shown represent every occurrence of a requested auto connect and the specific remote site where the connection was requested.

|                          |                                          |                        |
|--------------------------|------------------------------------------|------------------------|
| Date: mm/dd/yy           | IBM Sterling Connect:Enterprise for UNIX | Page 0001              |
| Time: hh:mm:ss           | Report Utility                           |                        |
| Command Line Parameters: |                                          |                        |
| cmureport                |                                          |                        |
| -sacq                    |                                          |                        |
| List                     | Start                                    | Remote Resource Status |
| xxxxxxx                  | yy/mm/dd-hh:mm:ss                        | xxxxxxx xxxxxxxx nnn   |
| xxxxxxx                  | yy/mm/dd-hh:mm:ss                        | xxxxxxx xxxxxxxx nnn   |
| xxxxxxx                  | yy/mm/dd-hh:mm:ss                        | xxxxxxx xxxxxxxx nnn   |
| xxxxxxx                  | yy/mm/dd-hh:mm:ss                        | xxxxxxx xxxxxxxx nnn   |

For each auto connect record, the following information is reported:

| Column   | Description                                                                                                                                    |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------|
| List     | The name listed in the ACD file for this session. If the ACD file name is longer than 8 characters, only the first 8 will be displayed.        |
| Start    | The date and time the auto connect was requested.                                                                                              |
| Remote   | The remote site where the request occurred.                                                                                                    |
| Resource | The resource(s) available to this auto connect.                                                                                                |
| Status   | A 4-digit failure code associated with a failed auto connect. Auto Connect Failure Codes are documented in Appendix A, <i>Error Messages</i> . |

## Offline Utilities Log Report

The Offline Utilities Log Report is designed to format detail records written to the log file by the command line utilities.

|                          |                                          |           |      |          |        |          |
|--------------------------|------------------------------------------|-----------|------|----------|--------|----------|
| Date: mm/dd/yy           | IBM Sterling Connect:Enterprise for UNIX | Page 0001 |      |          |        |          |
| Time: hh:mm:ss           | Report Utility                           |           |      |          |        |          |
| Command Line Parameters: |                                          |           |      |          |        |          |
| cmureport                |                                          |           |      |          |        |          |
| -soff                    |                                          |           |      |          |        |          |
| User                     | Start                                    | End       | Func | ID       | Bno    | Count    |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss  | xxx  | xxxxxxxx | nnnnnn | nnnnnnnn |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss  | xxx  | xxxxxxxx | nnnnnn | nnnnnnnn |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss  | xxx  | xxxxxxxx | nnnnnn | nnnnnnnn |
| xxxxxxxx                 | yy/mm/dd-hh:mm:ss                        | hh:mm:ss  | xxx  | xxxxxxxx | nnnnnn | nnnnnnnn |

Within the report body itself, each report contains these fields:

| Column | Description                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------|
| User   | The local user that issued the command.                                                             |
| Start  | The date and time when the process began.                                                           |
| End    | Time when the process ended.                                                                        |
| Func   | The mailbox function, such as <b>ADD</b> or <b>EXTRACT</b> , run on this batch during this process. |
| ID     | The mailbox ID of the batch.                                                                        |
| Bno    | The number of the batch processed.                                                                  |
| Count  | The size of the batch, in bytes.                                                                    |

## AS2 Report

To generate a report of the AS2 protocol activity, use the **as2report** utility.

Required parameters are in bold in the following table. All parameters (required or optional) can be input using either the abbreviated or long format. Unlike other Sterling Connect:Enterprise for UNIX command line utilities, the as2report utility does not allow spaces between a parameter and its values.

| Parameter                                                                                | Description                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-byyyymmdd[:hhmm] hhmm</b><br><b>--begin</b> <i>yyyymmdd[:hhmm] hhmm</i>              | Specifies the begin date and time the messages were transferred.                                                                                                                                                                                         |
| <b>-eyyyymmdd[:hhmm] hhmm</b><br><b>--end</b> <i>yyyymmdd[:hhmm] hhmm</i>                | Specifies the end date and time the messages were transferred.                                                                                                                                                                                           |
| <b>-f[']</b> <i>from name [']</i><br><b>--from</b> <i>['] from name [']</i>              | Specifies the from AS2 identifier of the AS2 contract.                                                                                                                                                                                                   |
| <b>-h</b><br><b>--help</b>                                                               | Print usage information.                                                                                                                                                                                                                                 |
| <b>-mcolumn delimiter</b><br><b>--delimit</b> <i>column delimiter</i>                    | Specifies the delimiter to use to separate columns. If the delimiter is not specified, column fields will be printed fixed width. For more information about the <b>-m</b> parameter, refer to <i>Displaying Pipe-Delimited AS2 Reports</i> on page 163. |
| <b>-n[']</b> <i>contract ID [']</i><br><b>--contract</b> <i>['] contract ID [']</i>      | Specifies the contract ID associated with the AS2 transfer.                                                                                                                                                                                              |
| <b>-rinbound outbound both</b><br><b>--direction</b> <i>inbound outbound both</i>        | Specifies the direction of the AS2 transfer from Sterling Connect:Enterprise.                                                                                                                                                                            |
| <b>-ssuccess failed pending all</b><br><b>--status</b> <i>success failed pending all</i> | Selects the status the AS2 message.                                                                                                                                                                                                                      |
| <b>-t[']</b> <i>to name [']</i><br><b>--to</b> <i>['] to name [']</i>                    | Specifies the to AS2 identifier of the AS2 contract.                                                                                                                                                                                                     |
| <b>-x</b><br><b>--xml</b>                                                                | Specifies to generate the output in xml format.                                                                                                                                                                                                          |

### Displaying Pipe-Delimited AS2 Reports

In addition to standard report formats, you can use the as2report utility to produce details into a pipe-delimited output. You can create custom reports by parsing this output. The following command produces all session details for the date range specified in a pipe-delimited format:

```
as2report -m"|" -byyyymmdd[:hhmm]|hhmm -eyyyymmdd[:hhmm]|hhmm
```

The output of this command is 21 pipe-delimited fields. Following is an example:

```
outbound|2005-04-01T11:52:29|outbound|SENT|122523|2005-04-01T11:52:29|122523|2005-04-01T11:52:30|122523|2005-04-01T11:52:29|1|"contract"|"batch.PL.24.RQ"|"batch.PL.24.MD"|"batch.PL"|"hostname1.com-1bdb58-102fee47e89--8000@hostname2.com"|"remote"|"local"|"hostname1.com-1bdb58-102fee47e89--7ffremote@hostname2.com"|"processed"|
```

The following table, organized by field position, describes each field in the output:

| Field Position | Description                                                               | Example Field                                               |
|----------------|---------------------------------------------------------------------------|-------------------------------------------------------------|
| 1              | Direction - outbound inbound                                              | outbound                                                    |
| 2              | Payload Creation Date and time                                            | 2005-04-01T11:52:29                                         |
| 3              | Mailbox name                                                              | outbound                                                    |
| 4              | Status                                                                    | SENT                                                        |
| 5              | AS2 Batch number (RQ batch)                                               | 122523                                                      |
| 6              | RQ Creation Date and time                                                 | 005-04-01T11:52:29                                          |
| 7              | MDN Batch Number                                                          | 122527                                                      |
| 8              | MDN Creation Date and time                                                | 2005-04-01T11:52:30                                         |
| 9              | Payload Batch Number                                                      | 122522                                                      |
| 10             | Payload Creation Date and time                                            | 2005-04-01T11:52:29                                         |
| 11             | Attempts to send                                                          | 1                                                           |
| 12             | AS2 contract name                                                         | "contract"                                                  |
| 13             | AS2 batch message name                                                    | "batch.PL.14.RQ"                                            |
| 14             | MDN batch name                                                            | "batch.PL.14.MD"                                            |
| 15             | Original (payload) batch name                                             | "batch.PL"                                                  |
| 16             | AS2 message ID                                                            | "hostname1.com-1bdb58-102fee47e89--8000@hostname2.com"      |
| 17             | Remote trading partner id                                                 | "remote"                                                    |
| 18             | Local trading partner id                                                  | "local"                                                     |
| 19             | MDN Message ID                                                            | "hostname1.com-1bdb58-102fee47e89--7ffscooby@hostname2.com" |
| 20             | Disposition                                                               | "processed"                                                 |
| 21             | Disposition modifier. This field only has a value if the MDN is negative. | ""                                                          |

---

# Configuring Secure FTP

Sterling Connect:Enterprise Secure FTP is a Secure FTP server and client using Secure Sockets Layer (SSL), a protocol that provides secure communications with transport protocols, including FTP over TCP/IP. It is an open, nonproprietary Internet protocol that has been widely adopted as standard. Sterling Connect:Enterprise Secure FTP ensures point-to-point security, meaning that the data is secured as it is transmitted across a single socket. To use Sterling Connect:Enterprise Secure FTP, both the sending and receiving sites must have FTP software that has SSL capabilities.

---

## Sterling Connect:Enterprise Secure FTP Features

Sterling Connect:Enterprise Secure FTP provides the following security features:

- ◆ **Secrecy**—Data is encrypted (scrambled) for privacy so that only the sender and recipient of the encrypted data can know its contents.
- ◆ **Authentication**—The client can determine that the entity that claims to be the server is really the server. Optionally, the server can authenticate the client.
- ◆ **Integrity (also known as reliability)**—The client and the server can determine whether the data has been modified in transit.

---

## Cryptography

To describe the security provided by Sterling Connect:Enterprise Secure FTP, it is necessary to introduce some of the basic concepts and terms of cryptography. This is a very high-level overview. For more complete understanding of security, refer to industry publications or the Internet.

Several key elements are required for Sterling Connect:Enterprise Secure FTP to provide security. Collectively, these elements are called cipher suites. Cipher suites are composed of the following:

- ◆ Key-exchange method
- ◆ Digital certificate type
- ◆ Message digest function
- ◆ Data encryption method

Cryptographic algorithms transform a plain text (readable) message into an encrypted form (called cipher text) that cannot be read by someone who is not intended to read it. The encrypted text can be converted to a readable form using a key.

The key-exchange method of a cipher suite is the mechanism the two communicating parties use to make these keys available to each other so they can communicate in private.

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.

### **Sterling Connect:Enterprise Secure FTP Client-Server Session**

Sterling Connect:Enterprise Secure FTP makes use of both types of cryptography. A client-server session begins with a handshake sequence containing the following:

- ◆ Client obtains server's public key (using certificates, explained below).
- ◆ Client generates a symmetric session key and sends a message to the server, encrypted with the server's public key, containing the session key.
- ◆ Server decrypts this message with its private key to obtain the session key.
- ◆ Client and server use the session key to encrypt and decrypt the rest of the transmitted data.

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

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

### **Authentication**

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 server's public key 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.

Sterling Connect:Enterprise Secure FTP enables CSR generation with the **cmusslgencsr** command. Sterling Certificate Wizard is also available to generate CSRs using a GUI. Manual interaction is required with third-party CAs, usually by E-mail, for the request, distribution, and installation of certificates.

Sterling Connect:Enterprise Secure FTP enables server authentication with the **cmusslverify** command. See the *IBM Sterling Connect:Enterprise for UNIX User's Guide* for more information about the **cmusslgencsr** and **cmusslverify** commands.

---

## Configuring Secure FTP

Complete the procedures in this section to configure Secure FTP.

### Establishing the Security Policy

Before your company can use Sterling Connect:Enterprise Secure FTP, you must determine the security needs of your various sites and those of your trading partners. After you establish the security policy, you must obtain the documents required to implement the security policy. Use the following procedure:

#### 1. Determining Your Company's Security Policy

Your security policy determines the overall security level you need to establish for your company. When deciding your overall policy, you should take into account your own requirements as well as those of your trading partners.

Your company's security policy can be set for all remote sites or on a site-by-site basis. You can create multiple Security Protocol Definition (SPD) files to have more than one set of security requirements. These files are created and modified using the Site Administration user interface.

#### 2. Establish the **Security Policy** for your remote sites. You have the following choices when setting your security policy:

- ◆ **Required**—All FTP transfers must be authenticated with Secure FTP.
- ◆ **Optional**—FTP transfers are authenticated when possible, but a transfer does not fail if the remote site does not have Secure FTP capabilities.
- ◆ **Disallowed**—Secure FTP transfers are not allowed.
- ◆ **Implicit**—Implies a value of “required” for all incoming FTP transfers. The FTP server instance will expect the SSL negotiation to begin immediately after the TCP/IP socket connection for the command socket. If the FTP client fails to immediately begin SSL negotiation, the connection will be closed with no feedback to the client.

3. Select **Minimum Security Protocol**: TLSv1 or SSLv3
4. Decide what **Cipher Strength** to use for you remote sites. Ensure that your cipher strength setting corresponds to the cipher strength setting of your remote sites. You have the following choices when setting your cipher strength:
  - ◆ **Strong suites only**—Secure FTP transfers are only performed with cipher suites that use strong encryption.
  - ◆ **Export suites only**—Secure FTP transfers are only performed with cipher suites that use export encryption.
  - ◆ **Allow all suites**—Secure FTP transfers are allowed with any cipher suite.
5. Decide what **Cipher Suites** to use for your remote sites.

Sterling Connect:Enterprise allows you to set a list of cipher suites for each SPD file. The cipher suites should be set in descending order with the most preferred suite listed first. Transfers between your Sterling Connect:Enterprise host and other Sterling Connect:Enterprise or Sterling Connect:Mailbox for UNIX servers must negotiate cipher suites between your list and the remote's list of cipher suites. The cipher suite used for the transfer is the first suite in the remote's list that matches a suite in your list. The cipher suite can appear anywhere in your list, thus the remote server always has control over which cipher suite is preferred.

---

**Note:** Sterling Connect:Enterprise Command Line Client (Secure FTP) and Sterling Connect:Enterprise Secure Client cannot specify cipher suites, only cipher strength.

---

The following cipher suites are supported by Sterling Connect:Enterprise Secure FTP:

| Strength                           | Ciphers                                                                                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Strong                             | RSA_WITH_AES_256_CBC_SHA<br>RSA_WITH_AES_128_CBC_SHA<br>RSA_WITH_3DES_EDE_CBC_SHA<br>RSA_WITH_RC4_128_SHA<br>RSA_WITH_RC4_128_MD5<br>RSA_WITH_DES_CBC_SHA |
| Export suites                      | RSA_EXPORT_WITH_RC4_40_MD5<br>RSA_EXPORT_WITH_DES40_CBC_SHA<br>RSA_EXPORT_WITH_RC2_CBC_40_MD5                                                             |
| Clear text with certificate suites | RSA_WITH_NULL_SHA<br>RSA_WITH_NULL_MD5                                                                                                                    |

6. Decide if you will require client authentication. By default, a remote client will authenticate the server. You can also authenticate the client before allowing a connection. To perform client authentication, you will need a certificate from each client you are authenticating and a trusted certificate that identifies them.
7. Decide what your clear channel control (CCC) policy will be. The following table describes your options.



| Strength              | Ciphers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL server CCC policy | <p>Specifies whether the FTP server accepts the Clear Control Channel (CCC) command if it is sent by the client. Each endpoint of the session must support use of the CCC command.</p> <p>Disallowed = Default. CCC is not attempted.</p> <p>Required = CCC must be accepted for the session.</p> <p>Optional = CCC is attempted. If rejected, the session remains connected and encrypted.</p>                                                                                                       |
| SSL client CCC policy | <p>Specifies whether an FTP automatic connection attempts to send the Clear Control Channel (CCC) command. If the command is accepted, the control connection operates in clear text for the remainder of the session. Each endpoint of the session must support use of the CCC command.</p> <p>Disallowed = Default. CCC is not attempted.</p> <p>Required = CCC must be accepted for the session.</p> <p>Optional = CCC is attempted. If rejected, the session remains connected and encrypted.</p> |

## Obtaining and Installing Your Certificate

Use the following procedure to obtain and install your certificate:

1. Select a Certificate Authority. A Certificate Authority (CA) is a company responsible for verifying and processing certificate requests, and issuing and managing certificates. The CA you choose should be one that your trading partners trust. Verisign ([www.verisign.com](http://www.verisign.com)) and Thawte ([www.thawte.com](http://www.thawte.com)) are CAs. You must meet the requirements of the CA you choose.
2. Run the **cmusslcust** script. This script is normally run as part of the Sterling Connect:Enterprise base installation. If you have already installed Sterling Connect:Enterprise for UNIX version 2.2, run **cmusslcust** from a command prompt.

In the **cmusslcust** script, you perform the following steps:

- a. Create a private key. The private key is automatically created by the script. You can encrypt your private key with a password for additional security. You can also choose a specific length for your private key.
- b. Generate a Certificate Signing Request (CSR).

A CSR contains the following information:

- Country Code—A 2-letter code that identifies the country in which your company is located. For example, the code for the United States is US.
- State/Province—Name of the state or province in which your company is located.
- City/Locality—Name of the city or locality in which your company is located.
- Organization Name—Name of your company.
- Organizational Unit—A subdivision or work-unit name within your company.
- Common Name—The server host name, or common name, must clearly identify the server and the company to remote partners. A remote site should be able to resolve this name to the IP address of your server.

- c. Set your security policy. Because you do not have your certificate installed on your host workstation, set your security policy to **Disallowed** or **Optional**. DO NOT set your security policy to **Required**. Doing so causes all attempted Sterling Connect:Enterprise FTP, both standard FTP and Secure FTP, transfers to fail.
  - d. Create a placeholder for your Key/Cert file. You create your Key/Cert file after you receive your certificate. Refer to step for instructions.
3. Purchase a certificate. When submitting a Certificate Signing Request (CSR), you can use the CSR created during the SSL configuration of the installation script, you can create a CSR using the **cmusslgencsr** command, or you can use a format directly from your CA. Submit your CSR to your CA in the manner specified by your CA. After your CA has verified the information in the CSR, you receive a certificate file.

---

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

---

4. Make a backup copy of your certificate. You always want to have a backup copy of your certificate file. 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.
5. Install your CA's trusted root certificate. The trusted root certificate for VeriSign and Thawte is included with Sterling Connect:Enterprise in the file *\$CMUHOME/spd/trusted.txt*. All other trusted roots must be obtained from the CA and added to the trusted root file. If you intend to communicate with sites running Sterling Connect:Enterprise for UNIX, Sterling Connect:Mailbox for UNIX, Sterling Connect:Enterprise Command Line Client (Secure FTP), or Sterling Connect:Enterprise Client for Microsoft Windows (Secure FTP), those sites also need the trusted root certificate from your CA.

Your trusted root certificate file should not contain more than one certificate for each CA. Superseded or expired root certificates should be removed.

6. Create your Key/Cert file. The Key/Cert file is created by concatenating your certificate to your private key. Following is an example:

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

7. Use the **cmusslverify** command to verify your Key/Cert file.
8. Make a secure backup copy of your Key/Cert file. You always want to have a backup copy of your Key/Cert file. This file can become corrupted or can be accidentally deleted. If you lose your Key/Cert 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.
9. Create your security protocol definition. Using the Site Administration user interface, create as many security protocol definitions as needed for Secure FTP communications with your remote sites. For each security protocol definition, set the parameters as determined in the first section of this worksheet.
10. After you install your certificate on the host workstation, reset the **Security Policy** parameter as needed.

11. Set the **Security protocol file** parameter in your schedule, communications protocol, and account definition files as needed. The **Security protocol file** parameter specifies which security protocol definition is used for an individual remote site or an schedule. Refer to the *IBM Sterling Connect:Enterprise for UNIX Web Administration User Interface Help* for instructions.

---

**Note:** The CPD **Security protocol file** parameter was set by the **cmusslcust** script. The value of the CPD **Security protocol file** parameter is the global default setting for Sterling Connect:Enterprise Secure FTP transfers.

---



---

# Configuring SSHFTP Protocol

SSH is a client-server architecture used to securely connect over a network. There are three components that make up the SSH Client protocol:

- ◆ SSH—used as a secure Telnet
- ◆ SCP—used for secure file copy
- ◆ SFTP—used for secure FTP transactions

The Sterling Connect:Enterprise for UNIX SSH server support SFTP and SCP clients. Use the information in this appendix to configure communication between Sterling Connect:Enterprise for UNIX and SSHFTP clients.

---

## Configuring Sterling Connect:Enterprise SSH Server

During installation, you have the opportunity to configure SSH. If you elect to configure SSH, the installation script calls the SSH customization script. If you elect not to configure SSH during installation, you can run the following SSH customization script, located in the \$CMUHOME/etc/ directory.

```
cmusshcust
```

You will need the following information:

| Information Required | Description                                                                               | Where to put the information                                                                                                                                                                                              |
|----------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSHFTP listener port | Select the secure FTP port that the SSHFTP daemon will monitor for incoming SSH requests. | Specify this value when prompted during the installation or when running the cmusshcust script. If you need to change this port number, use the Define Communications function of the Site Administration user interface. |

| Information Required                                                        | Description                                                                                                                                                    | Where to put the information                                                                    |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Type of host key to use for the Sterling Connect:Enterprise for UNIX server | Sterling Connect:Enterprise for UNIX supports both RSA and DSA keys for SSH.                                                                                   | Specify this value when prompted during the installation or when running the cmusshcust script. |
| Number of bits to use in the host key                                       | The host key can be anywhere from 512 to 32768 bits. The larger the key, the greater the security. Some clients and servers cannot use keys greater than 2048. | Specify this value when prompted during the installation or when running the cmusshcust script. |

The SSH customization script creates the SSH public host key as:

```
$CMUHOME/ssh/system/ssh_host_key.pub
```

Provide this key to your client.

The SSH customization script creates the private host key as:

```
$CMUHOME/ssh/system/ssh_host_key
```

Do not share this key.

## Configuring a Remote SSHFTP Client Connection

When configuring the connection between a remote client and Sterling Connect:Enterprise SSH server, you can configure to use password authentication or public key authentication. Your choice for authentication determines how you configure your protocol definition and account definition. Use the following procedure:

1. Decide on the authentication routine for SSH. Use the following table as a guide:

| If you want this authentication routine                                                                                                                                 | Set this in the communication definition                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Sterling Connect:Enterprise only performs password authentication.                                                                                                      | Password authentication = Yes<br>Public key authentication = No  |
| Sterling Connect:Enterprise only performs public key authentication.                                                                                                    | Password authentication = No<br>Public key authentication = Yes  |
| Sterling Connect:Enterprise first attempts public key authentication. If public key authentication fails, Sterling Connect:Enterprise attempts password authentication. | Password authentication = Yes<br>Public key authentication = Yes |

2. Decide if you will allow remote users to issue Secure Copy (SCP) commands.
3. Decide what Ciphers you allow for encryption.
4. Decide what Message Authentication Codes (MACs) you will allow for message integrity protection. Also decide on the order of preference.
5. Provide your server requirements for authentication, Ciphers, and MACs to your clients.
6. Use the Define Communications function of the Site Administration user interface to setup the SSHFTP protocol definition based on step 1 on page 174 through step 4 on page 175.





---

# Configuring AS2

This chapter provides information on using Sterling Connect:Enterprise for UNIX to exchange data with a trading partner using the AS2 transport protocol. Read this information and complete the procedures described in this chapter before attempting to implement AS2 using the Sterling Connect:Enterprise for UNIX Site Administration user interface.

Use the worksheets in this chapter to gather configuration information from your trading partner and from the system administrator at your local site. Refer to the completed worksheets when you are using the Sterling Connect:Enterprise for UNIX Site Administration user interface to set up the AS2 contract before you begin exchanging data.

---

## About AS2

Applicability Standard 2 (AS2) is a transport protocol that uses HTTP to transport data over the Internet. It offers a flexible set of security options for organizing the transfer of data between companies. These options include using a secure HTTP connection and S/MIME for data privacy, data integrity, data authenticity, and nonrepudiation.

Implementing AS2 requires you to agree with your trading partner on security options, including signing, encryption, and Message Delivery Notification (MDN) options. You will also need to exchange AS2 identifiers, certificates for S/MIME and SSL (HTTPS) and information about the HTTP URLs and ports that each of you will be using for the exchange.

The following diagrams illustrates how Sterling Connect:Enterprise sends and receives data and how different types of batches are created (PL, RQ, MD, OK, NM, BD, AS2, and BQ). These diagrams assume all security measures and message options are being used.

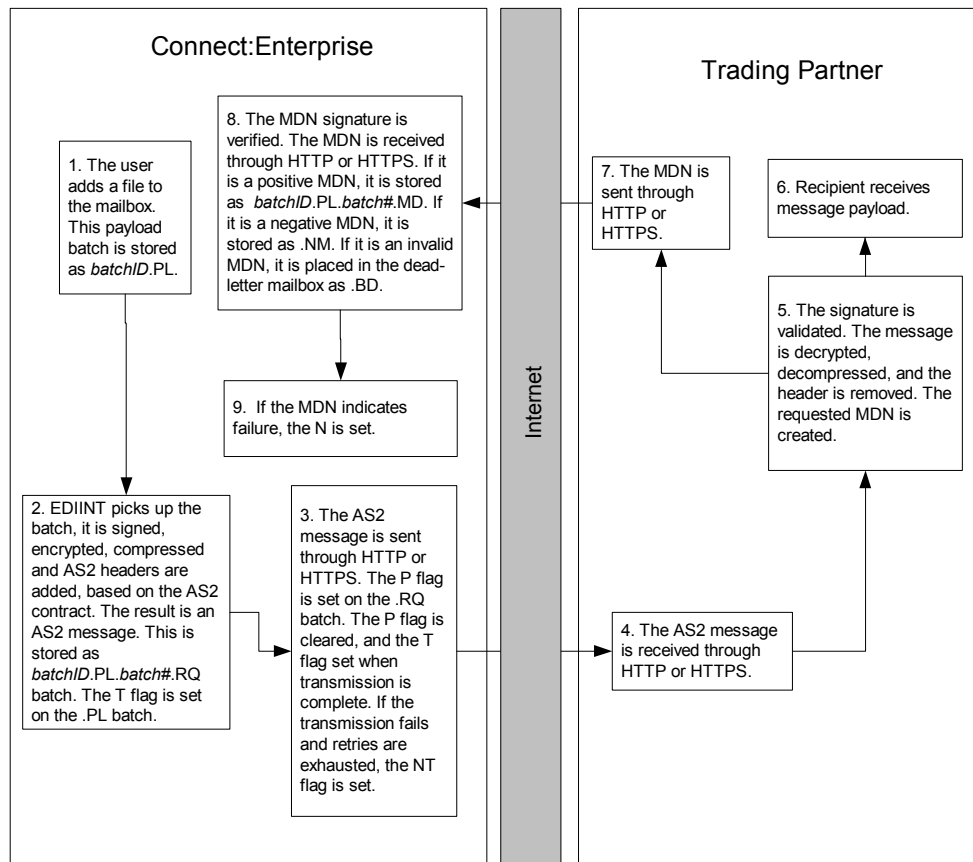
## Sending from Sterling Connect:Enterprise to a Trading Partner

The following diagram illustrates the process when sending batches from Sterling Connect:Enterprise to a trading partner. This process involves the \*.PL, \*.RQ, \*.MD, \*.NM, and \*.BD batch suffixes.

---

**Note:** The \*.PL suffix is configurable in the schedule definition. It is the payload to be sent.

---




---

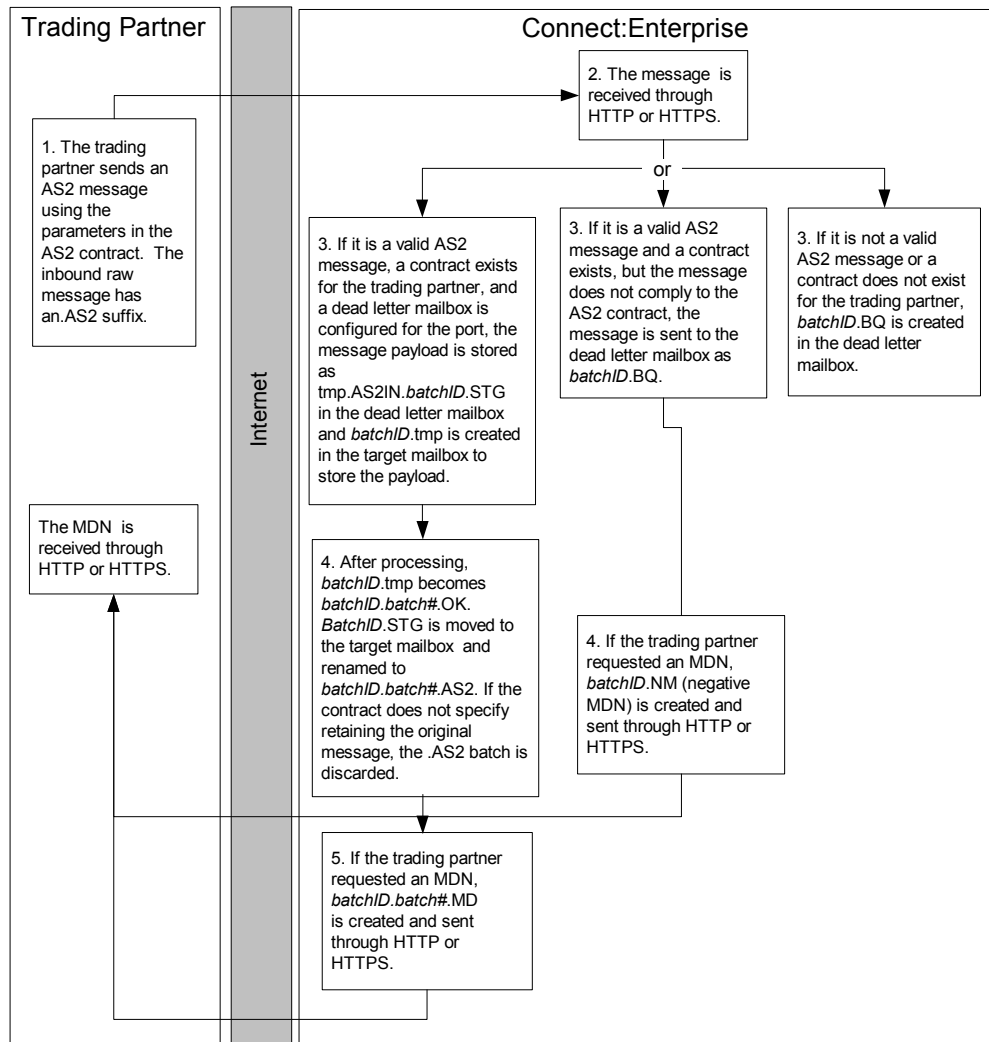
**Note:** Not all batches referred to in these diagrams are always created. If the “retain original message in recipient mailbox” option is not enabled, the .AS2 batch is not saved for inbound messages and the .MD batch is not saved for outbound messages.

---

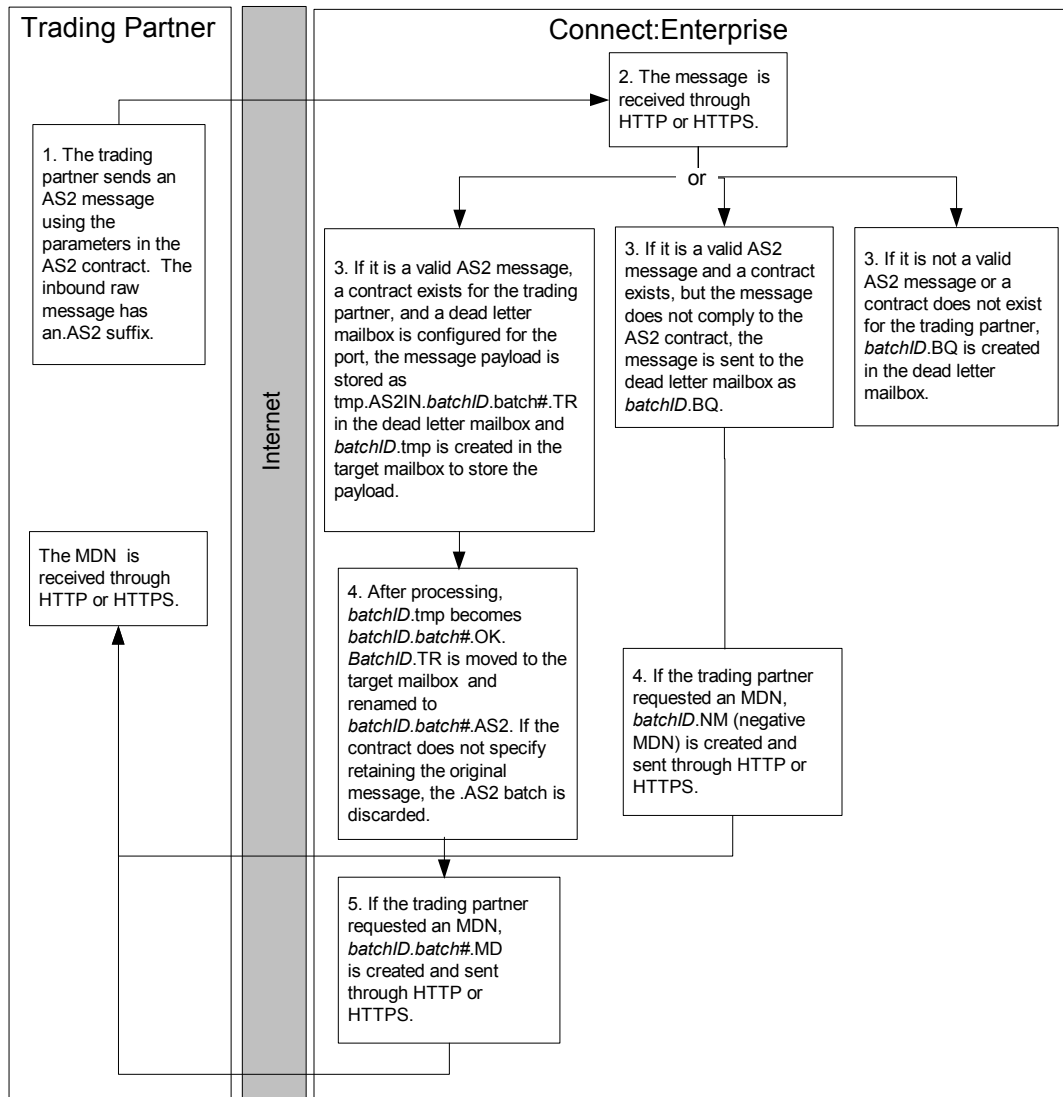
## Receiving AS2 Messages from a Trading Partner

The following diagrams illustrate the process when receiving batches from a trading partner. This process involves the \*.STG, \*.TR, \*.TMP, \*.OK, \*.MD, \*.NM, and \*.BQ batch suffixes.

### AS2 Messages Requesting Async MDNs



## AS2 Messages Requesting Sync MDNs



Duplicate messages are usually not processed and stored in the target mailbox, but if the original MDN batches have been erased, the duplicate must be reprocessed to create a new MDN response. In this case, a new MDN batch will be created with the appropriate .MD or .NM suffix. The .AS2 and .OK batches will also be created but with an additional .dup suffix indicating they are duplicates.

## Configuring Sterling Connect:Enterprise for UNIX for AS2

If you did not configure AS2 during installation, use the following procedure:

1. Navigate to the \$CMUHOME/etc directory and run the **as2cust** utility. This will complete the AS2 customization. Following is an example:

```

=====
IBM(R) Sterling Connect:Enterprise(R) for UNIX
(C) Copyright IBM Corp. 1994, 2011 All Rights Reserved.
IBM and the IBM logo are Trademarks of International Business Machines
version 2.5.00 Customization

This customization procedure sets up AS2 for IBM(R) Sterling
Connect:Enterprise(R) for UNIX
operating environment.

As a shorthand, entering ENTER at the prompt means use the default value, if any.
To abort the process, enter Control-C.
=====

Press ENTER when ready.

Using Java Runtime "/data/ahmi_ce2402/jre/bin/java"

/data/ahmi_ce2402/javalib/cmuhhttpd saved as
/data/ahmi_ce2402/javalib/cmuhhttpd.2011.03.01.19.17

Created script: /data/ahmi_ce2402/javalib/cmuhhttpd

/data/ahmi_ce2402/javalib/cmuediintd saved as
/data/ahmi_ce2402/javalib/cmuediintd.2011.03.01.19.17

Created script: /data/ahmi_ce2402/javalib/cmuediintd

Created script: /data/ahmi_ce2402/javalib/as2report

Created script: /data/ahmi_ce2402/javalib/as2delete

An existing AS2 configuration file has been found and will not
be overwritten or modified.
The file path is: /data/ahmi_ce2402/as2/AS2-Configuration.xml

AS2 Customization Completed

```

2. Start the HTTP daemon (**cmuhhttpd**) and the EDIINT daemon (**cmuediintd**). Refer to Chapter 5, *Starting and Stopping Sterling Connect:Enterprise*, for more information.

## Configuring the AS2 Port

The AS2 port receives incoming AS2 messages. You specify the URL and port numbers and the SSL requirements. Use the following worksheet to gather the information to set up the AS2 port. You then define the port using the Sterling Connect:Enterprise for UNIX Site Administration user interface.

| Information Required                                 | Description                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP address or host name accessible from the Internet | IP address that you want trading partners to send AS2 messages to.                                                                                                                                                                                                                                                                        |
| AS2 listening port                                   | Port that you want AS2 to listen on.                                                                                                                                                                                                                                                                                                      |
| Translated listening port                            | Port that the AS2 listener port is mapped to when using network address translation.                                                                                                                                                                                                                                                      |
| Dead-letter mailbox:                                 | Mailbox where invalid requests and invalid MDNs are stored. If blank, these requests and MDNs are not stored.                                                                                                                                                                                                                             |
| Cipher strength                                      | Cipher strength to be used for SSL. Options are:<br>None = Default<br>Strong = Allow only cipher suites with greater than 40-bit encryption.<br>All = Allow strong and weak cipher suites. Weak cipher suites use 40-bit encryption.<br>Custom = Use specific cipher suites.<br>If you select Custom, you must specify the cipher suites. |
| Cipher suites                                        | If you select Custom as the cipher strength, you must specify the cipher suites to use.                                                                                                                                                                                                                                                   |
| Key certificate file                                 | Specifies the location of the key certificate file containing the private key for SSL server authentication.                                                                                                                                                                                                                              |

After you define an AS2 port for Sterling Connect:Enterprise for UNIX, you must give your URL to the AS2 trading partner that connects to your system. The URL that they use must have the following format:

```
http://hostname:port/as2/mailboxid/batchid
or
https://hostname:port/as2/mailboxid/batchid for SSL connections
```

as2 is required and must be in lowercase letters, mailboxid is the mailbox that you want the inbound batches to go to, and batchid is the batch ID that you want to assign the AS2 message.

---

## Configuring the HTTP Proxy

An HTTP proxy may be required to send AS2 messages. You specify the proxy servers you want to use to send AS2 messages. For each proxy server, you define URLs or URL patterns (using regular expression). If a URL matches, it uses this proxy for outbound requests. Use the following worksheet to gather information.

| Information Required | Description                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------|
| Proxy server URL     | Required. Specifies the URL for the HTTP proxy.                                                                        |
| User ID              | If required, specifies the user ID needed to access the proxy server URL.                                              |
| Password             | If required, specifies the password needed to access the proxy server URL.                                             |
| URL                  | Specifies the URL that will be mapped to the proxy you are defining. You can use regular expression to identify a URL. |

---

## Creating the AS2 Contract

After you define the port and proxy information, the next step is to create the contracts. Use the worksheets in this section to gather the information necessary to create your AS2 contracts.

### Identity Information Worksheet

Use the following worksheet to gather identity information for you and your trading partner.

| Information Required                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>What your trading partner needs from you</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Local AS2 identifier                            | Required AS2 identifier that you want your trading partner to use to identify you.                                                                                                                                                                                                                                                                                                                                                                      |
| Local AS2 URL                                   | Required. URL you want your trading partner to send AS2 message to. It must be in the following format:<br><code>http://hostname:port/as2/mailbox_ID/batch_ID</code><br>where <i>hostname</i> , <i>port</i> , and <i>mailbox_ID</i> identify where you want your trading partner to send to and <i>batch_ID</i> identifies the name they must give the batch they are sending. If it is a secure port, this URL must begin with <code>https://</code> . |

| Information Required                           | Description                                                                          |
|------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>What you need from your trading partner</b> |                                                                                      |
| AS2 identifier for remote trading partner      | Required AS2 identifier that your trading partner wants you to use to identify them. |
| Remote trading partner URL                     | Required URL your trading partner wants you to use to send AS2 messages.             |
| User ID                                        | User ID you need if required by the URL your trading partner provides.               |
| Password                                       | Password you need if required by the URL your trading partner provides.              |

## SSL Information Worksheet

You may need to negotiate some of these settings with your trading partner.

| Information Required                                           | Description                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>What your trading partner needs from you</b>                |                                                                                                                                                                                                                                                                                                       |
| Direct trust certificate or trusted root                       | Provide a direct trust certificate file to your trading partner or a trusted root certificate.                                                                                                                                                                                                        |
| Cipher strength for SSL                                        | Options are:<br>None = Default<br>Strong = Allow only cipher suites with greater than 40-bit encryption.<br>All = Allow strong and weak cipher suites. Weak cipher suites use 40-bit encryption.<br>Custom = Use specific cipher suites.<br>If you select Custom, you must specify the cipher suites. |
| Common name validation                                         | If your trading partner wants to use common name validation, they need the common name from your certificate, which depends on your specific common name policy.                                                                                                                                      |
| <b>What you need from your trading partner</b>                 |                                                                                                                                                                                                                                                                                                       |
| Direct trust certificate file or trusted root certificate file | Acquire the trusted root certificate file or a direct trust certificate from your trading partner and specify the path and file name where it is saved. This file is used to authenticate your trading partner during SSL negotiations.                                                               |



| Information Required    | Description                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cipher strength for SSL | <p>Cipher strength to be used for SSL. Options are:</p> <p>None = Default</p> <p>Strong = Allow only cipher suites with greater than 40-bit encryption.</p> <p>All = Allow strong and weak cipher suites. Weak cipher suites use 40-bit encryption.</p> <p>Custom = Use specific cipher suites.</p> <p>If you select Custom, you must specify the cipher suites.</p> |
| Common name validation  | <p>If you want to use common name validation, you need the common name from your trading partner certificate. This will depend on your specific common name policy. You can validate on:</p> <p>Host name</p> <p>DNS name</p> <p>Other (specify)</p>                                                                                                                 |

## Digital Signature Information Worksheet

If you are signing messages or authenticating signed messages, use the following worksheet to collect certificates and algorithm requirements for your local site and your trading partner. You may need to negotiate some of these settings with your trading partner.

| Information Required                            | Description                                                                                                                                    |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>What your trading partner needs from you</b> |                                                                                                                                                |
| Signing certificate file                        | Signing certificate to authenticate messages that you send.                                                                                    |
| <b>What you need from your trading partner</b>  |                                                                                                                                                |
| Signing certificate file:                       | Acquire the signing certificate you use to authenticate your trading partner's signature and specify the path and file name where it is saved. |
| Signing algorithm:                              | Signing algorithm that your trading partner requires you to use when signing messages.                                                         |

## Exchange Encrypted Messages Information Worksheet

Use the following worksheet to collect certificates and algorithm requirements for your local site and your trading partner when you require encrypted messages. You may need to negotiate some of these settings with your trading partner.

| Information Required                            | Description                                                                                         |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>What your trading partner needs from you</b> |                                                                                                     |
| Exchange algorithm                              | Exchange algorithm that you require your trading partner to use to encrypt messages.                |
| Exchange certificate                            | Public exchange certificate that your trading partner must use to encrypt messages to send to you.  |
| <b>What you need from your trading partner</b>  |                                                                                                     |
| Exchange algorithm                              | Exchange algorithm that your trading partner requires you to use when encrypting messages.          |
| Exchange certificate file                       | Public exchange certificate that your trading partner requires you to use when encrypting messages. |

### Message Options Worksheet

Use the following table to collect message option preferences for your local site and your trading partner.

| Information Required                               | Description                                                                                                                                      |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>What you need from your trading partner</b>     |                                                                                                                                                  |
| MIME type/subtype                                  | Specific MIME type/subtype your trading partner requires, if any.                                                                                |
| Compress message                                   | If your trading partner requires you to compress message.                                                                                        |
| <b>What you need to decide for your local site</b> |                                                                                                                                                  |
| Port to receive asynchronous MDN                   | Port available to receive asynchronous MDNs (HTTP or HTTPS). This can be the same port that receives AS2 messages.                               |
| MDN type                                           | Type of MDN you want to receive. If Asynchronous (returns on a different communication channel that the message was sent), specify a port.       |
| To request a signed MDN, specify the algorithm     | Signing algorithm you want your trading partner to use when signing MDNs.                                                                        |
| Number of retries for failed attempts              | Number of times an attempt to retransmit the message will be made before the request is failed. This field only applies when you are using MDNs. |
| Time out                                           | The time allowed for a message to be transmitted and the corresponding MDN to be returned. This field only applies when you are using MDNs.      |

---

## Retry of Outbound AS2 Connections

Use the information in this section to configure the retry attempts for AS2 messages.

### For AS2 Messages Requiring an MDN

Use the following procedure to establish the retry policy for outbound AS2 messages that require synchronous MDNs:

1. From the Site Administration user interface, click **Define AS2 Contract**.
2. From the Manage AS2 Contract screen, select the contract you want to configure the retry settings and click **Edit**.
3. At the top of the screen click **MDN** to display the Configure MDN screen.
4. Specify **Number of retries for failed attempts** (the actual number of attempts is this number plus the initial connection attempt) and **Time out** values.
5. From the Site Administration user interface, click **Define Schedules**.
6. From the Manage Schedules screen, select the schedule you want to configure the retry settings and click **Edit** or click **New** to create a new schedule.
7. Define the schedule as needed to send your AS2 message. Delete any value from the **Times to requeue remote resource** and **Retry connection attempts** fields. This will ensure that the retry definition that is set in the AS2 contract (step 4) is used.

### For Outbound Asynchronous MDNs

By default, outbound asynchronous MDN will retry 5 times after the initial attempt at 5 minute intervals. If you need to change this value, use the following procedure:

1. From the Site Administration user interface, click **Define AS2 Contract**.
2. From the Manage AS2 Contract screen, select the contract you want to configure the retry settings and click **Edit**.
3. At the top of the screen click **Inbound** to display the Configure Inbound Message screen.
4. Note all mailboxes identified in the **Mailboxes trading partner can send to** field.
5. From a command line, navigate the \$CMUHOME/acd directory.
6. For each mailbox from the list of mailboxes from step 4, there is a *.mailbox.acd* file. Open the first file in the list.
7. Update the following parameters in the *.mailbox.acd* file as required:

```
INTERVAL = n
REQUEUES = n
```

8. Repeat step 6 and step 7 for each *.mailbox.acd* file in the list.

## For AS2 Messages Not Requiring an MDN

By default, for AS2 messages that require an asynchronous MDN will retry 9 times after the initial attempt at 30 second intervals. You cannot change this value.

---

# Configuring WebDAV Protocol

The Web-based Distributed Authoring and Versioning (WebDAV) protocol is a set of extensions that work within the HTTP protocol. These extensions allow you to manage and edit data that is located on remote Web servers. The Sterling Connect:Enterprise implementation of WebDAV allows you to exchange data with Sterling Connect:Enterprise using Microsoft Windows in the same way that you would any directory structure. You can also use any WebDAV client available with UNIX operating systems.

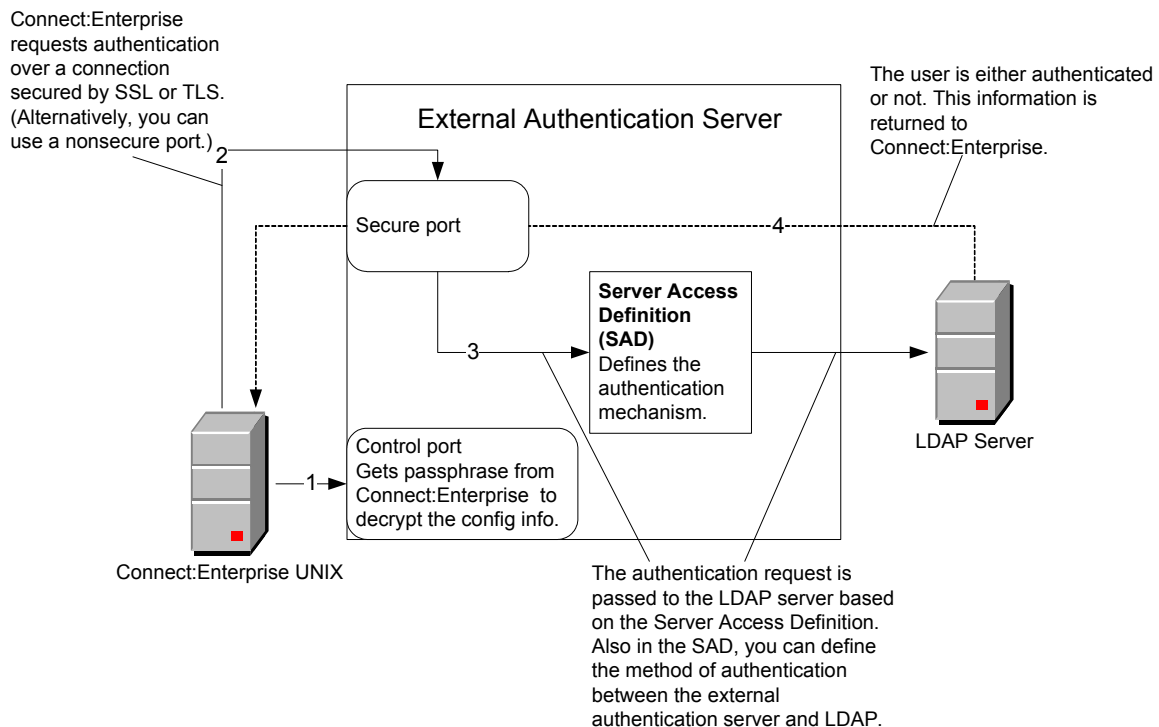
To configure the Sterling Connect:Enterprise WebDAV, you only need to configure the HTTP port for WebDAV. Use the Define Communications function of the Sterling Connect:Enterprise for UNIX Site Administration user interface to set up the WebDAV server. Information on Configuring a WebDAV port are in the Help for the Site Administration User Interface. The initial installation of the Sterling Connect:Enterprise WebDAV uses the same port at the Site Administration User Interface. You can add support for SSL (HTTPS) and additional ports.

You will need to provide the hostname and port number of your WebDAV server to any client that is connecting through WebDAV.



## Configuring the External Authentication Service

The external authentication service that is part of Sterling Connect:Enterprise serves as a proxy between Sterling Connect:Enterprise and an LDAP server. It allows you to authenticate users with your existing LDAP directory, rather than using the native authentication capability of Sterling Connect:Enterprise. The following diagram describes the basic architecture of the external authentication service:



To configure the external authentication service, you must have your LDAP server already installed and configured. Use the steps in this chapter to configure the connection between Sterling Connect:Enterprise and the external authentication service. After you establish this connection, use the Define Access and Define Access Groups functions of the Site Administration user interface to establish the Server Access Definition (SAD) and the connection between the external authentication service and your LDAP server.

---

## Determine What Procedures to Follow

If you plan to use a secure connection between Sterling Connect:Enterprise and the external authentication service, perform all procedures in this chapter (except those identified as optional) in the order they are presented. If you do not plan to use a secure connection between Sterling Connect:Enterprise and the external authentication service, refer to *Start Sterling Connect:Enterprise and the External Authentication Service* on page 198 and *Define the Server Access Definition* on page 202.

---

## Configuring the SSL Credentials for Connection

If you plan to use a secure connection between Sterling Connect:Enterprise and the external authentication service, use the procedures in this section.

### Specify the Path to Keytool

You must use the keytool utility that is part of the external authentication service. Use this procedure to ensure that you are using the appropriate keytool.

1. Type the following command to specify the path and press **Enter**:

For KSH:

```
export PATH=$CMUHOME/externalauth/IDMB/jre/bin:$CMUHOME/externalauth/IDMB/bin:$PATH
```

For CSH:

```
setenv PATH $CMUHOME/externalauth/IDMB/jre/bin:$CMUHOME/externalauth/IDMB/bin:$PATH
```

2. Type the following command to verify the keytool that you are using and press **Enter**.

```
which keytool
```

3. The system returns the path value. Verify that this path value is:

```
$CMUHOME/externalauth/IDMB/jre/bin
```



## Change the Default Passphrases for the External Authentication Service

The external authentication service is installed with default passwords for the keystore file and the truststore file, and the passphrase for the encryption key. If you intend to change the default values, you must perform this procedure before *Create a Key/Certificate for the External Authentication Service* on page 195 because the certificate and the truststore password must be the same.

1. Type the following command to change the encryption passphrase:

```
change passphrase.sh -x
```

2. You are prompted for the current passphrase. Type the current passphrase and press **Enter** (the initial value is *changeit*).
3. You are prompted for the new passphrase. Type the new passphrase and press **Enter**.
4. You are prompted to verify the new passphrase. Type the new passphrase again and press **Enter**.
5. Type the following command to change the keystore password:

```
keytool -storepasswd -v -new newpassword -keystore keystore_path -storepass password
```

The following table describes the command elements:

| Element                        | Description                                                                                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>keytool</b>                 | Invokes the keytool utility.                                                                                                                                                                                                                                         |
| -storepasswd                   | Instructs keytool to change the password.                                                                                                                                                                                                                            |
| -v                             | Instructs keytool to use verbose output.                                                                                                                                                                                                                             |
| -new <i>newpassword</i>        | Specifies the new password for the keystore.                                                                                                                                                                                                                         |
| -keystore <i>keystore_path</i> | Specifies the path and file name of the key store file. \$CMUHOME/externalauth/IDMB/conf/system/keystore is the default. If you use a value other than the default, you must update the sslinfo.xml with the new path and file name using the sslinfotool.sh script. |
| -storepass <i>password</i>     | Specifies the current password of the keystore file. The initial value is <i>password</i> .                                                                                                                                                                          |

6. Type the following command to change the truststore password:

```
keytool -storepasswd -v -new newpassword -keystore truststore_path -storepass changeit
```

The following table describes the command elements:

| Element                          | Description                                                                                                                                                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>keytool</b>                   | Invokes the keytool utility.                                                                                                                                                                                                                                            |
| -storepasswd                     | Instructs keytool to change the password.                                                                                                                                                                                                                               |
| -v                               | Instructs keytool to use verbose mode.                                                                                                                                                                                                                                  |
| -new <i>newpassword</i>          | Specifies the new password for the truststore.                                                                                                                                                                                                                          |
| -keystore <i>truststore_path</i> | Specifies the path and file name of the truststore file. \$CMUHOME/externalauth/IDMB/conf/system/truststore is the default. If you use a value other than the default, you must update the sslinfo.xml with the new path and file name using the sslinfotool.sh script. |
| -storepass <i>changeit</i>       | Specifies the current password of the truststore file. The initial value is <i>changeit</i> .                                                                                                                                                                           |

7. Type the following command to update the keystore and truststore passwords in the sslinfo.xml file to the ones you updated in steps step 5 on page 193 and step 6 on page 193:

```
sslinfotool.sh -p=passphrase -w=newkeystorepassword -W=newtruststorepassword
```

The following table describes the command elements:

| Element                          | Description                                                                                        |
|----------------------------------|----------------------------------------------------------------------------------------------------|
| <b>sslinfotool.sh</b>            | Invokes the sslinfotool.sh                                                                         |
| -p= <i>passphrase</i>            | Specifies the passphrase for the external authentication server you changed in step 1 on page 193. |
| -w= <i>newkeystorepassword</i>   | Specifies the new keystore password you changed in step 5 on page 193.                             |
| -W= <i>newtruststorepassword</i> | Specifies the new truststore password you changed in step 6 on page 193.                           |

The following message is displayed:

```
"$CMUHOME/externalauth/IDMB/conf/system/sslInfo.xml" updated successfully
```

## Create a Key/Certificate for the External Authentication Service

The certificate portion of the key/certificate is used to authenticate the external authentication service to Sterling Connect:Enterprise. Use the following procedure to generate a key/certificate and save it in the external authentication service keystore file.

1. From the `$CMUHOME/externalauth/IDMB/jre/bin` directory, type the following command:

```
keytool -genkey -alias alias_name -keyalg alg_type -keystore keystore_path
-storepass password
```

The following table describes the command elements:

| Element                        | Description                                                                                                                                                                                                                                                            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>keytool</b>                 | Invokes the keytool utility.                                                                                                                                                                                                                                           |
| -genkey                        | Instructs keytool to generate a certificate.                                                                                                                                                                                                                           |
| -alias <i>alias_name</i>       | Specifies the name of the certificate. This name will be in the certificate and will also be used to identify the certificate in the keystore.<br>You will also need this information when you <i>Enable the Secure Access Acceptor</i> on page 200.                   |
| -keyalg <i>alg_type</i>        | Specifies the type of algorithm used to create the key. This value must be RSA.                                                                                                                                                                                        |
| -keystore <i>keystore_path</i> | Specifies the path and file name of the key store file.<br>\$CMUHOME/externalauth/IDMB/conf/system/keystore is the default. If you use a value other than the default, you must update the sslinfo.xml with the new path and file name using the sslinfoool.sh script. |
| -storepass <i>password</i>     | Specifies the password of the keystore file. Use the value you specified in step 5 on page 193.                                                                                                                                                                        |

Following is an example:

```
$ keytool -genkey -alias externalauthkeycert -keyalg RSA -keystore
$CMUHOME/externalauth/IDMB/conf/system/keystore -storepass password
```

2. When prompted, supply the following information and press **Enter** after each prompt:
  - ◆ First and last name. Use a value that identifies the external authentication service, such as “External Authentication.”
  - ◆ Organizational unit
  - ◆ Organization
  - ◆ City or locality
  - ◆ State or Province (use CAPS)
  - ◆ Two letter country code (use CAPS)

3. When prompted, verify the information you provided and press **Enter**.
4. You are prompted with the following:

```
Enter key password for <alias_name>
(RETURN if same as keystore password):
```

**Do not type a password.** Press **Enter**. The key/certificate and keystore passwords must be the same for the external authentication service to function properly.

## Export the External Authentication Service Certificate to Sterling Connect:Enterprise

Use the following procedure to export the signed external authentication service certificate to Sterling Connect:Enterprise:

1. Type the following command:

```
keytool -export -alias alias_name -keystore keystore_path -storepass password
-file $CMUHOME/spd/cert_alias -rfc
```

The following table describes the command elements:

| Element                                   | Description                                                                                                                                                                                                                                                                                             |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>keytool</b>                            | Invokes the keytool utility.                                                                                                                                                                                                                                                                            |
| -export                                   | Instructs keytool to export the certificate.                                                                                                                                                                                                                                                            |
| -alias <i>alias_name</i>                  | Specifies the name of the certificate you created in <i>Create a Key/Certificate for the External Authentication Service</i> on page 195.                                                                                                                                                               |
| -keystore <i>keystore_path</i>            | Specifies the path and file name of the key store file. <code>\$CMUHOME/externalauth/IDMB/conf/system/keystore</code> is the default. If you use a value other than the default, you must update the <code>sslinfo.xml</code> with the new path and file name using the <code>sslinfo.sh</code> script. |
| -storepass <i>password</i>                | Specifies the password of the keystore file.                                                                                                                                                                                                                                                            |
| -file <code>\$CMUHOME/spd/filename</code> | Specifies the path and filename where you want to export the certificate to. The path will always be <code>\$CMUHOME/spd</code> .                                                                                                                                                                       |
| -rfc                                      | Formats the certificate in Privacy Enhanced Mail (PEM) format.                                                                                                                                                                                                                                          |

Following is an example:

```
$ keytool -export -alias externalauthkeycert -keystore
$CMUHOME/externalauth/IDMB/conf/system/keystore -storepass mypassword -file
$CMUHOME/spd/externalauthcertificate -rfc
```

## Create a Key/Certificate for Sterling Connect:Enterprise

If you already have a key/certificate for Sterling Connect:Enterprise, this procedure is not necessary. If you do not already have a key/certificate for Sterling Connect:Enterprise, you can use Sterling Certificate Wizard or `cmusslgencsr` to create a key/certificate. The following procedure demonstrates how to create a key/certificate using `cmusslgencsr`. The public portion of this key/certificate is used by the external authentication service to authenticate Sterling Connect:Enterprise.

1. Navigate to the `$CMUHOME/spd` directory.
2. Use the following command to create a certificate for Sterling Connect:Enterprise:

```
cmusslgencsr
```

3. When prompted, supply the following information and press **Enter** after each prompt:

- ◆ Two letter country code
- ◆ State or Province
- ◆ Organizational name
- ◆ Organizational unit
- ◆ Common name (server host name)

A private key (`privkey.txt`) and a Certificate Signing Request (`csr.txt`) are created in the `$CMUHOME/spd` directory.

4. To get your certificate signed by a CA, submit `csr.txt` according to the requirements of the CA.
5. After you get your signed certificate from the CA, use the following command to create a Key/Certificate for Sterling Connect:Enterprise:

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

where `cert.txt` is your signed certificate and `keycert.txt` the name for your key/certificate.

## Import the Sterling Connect:Enterprise Certificate to the External Authentication Service Truststore

Use this procedure to import the Sterling Connect:Enterprise CA certificate to the external authentication service. It will be used to authenticate the Sterling Connect:Enterprise server.

1. Navigate to the `$CMUHOME/externalauth/IDMB/jre/bin` directory and type the following command:

```
keytool -import -keystore truststore_path -storepass password -file certificate
```

The following table describes the command elements:

| Element                          | Description                                                                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>keytool</b>                   | Invokes the keytool utility.                                                                                                                                                                                                                                   |
| -import                          | Instructs keytool to import a certificate to the keystore.                                                                                                                                                                                                     |
| -keystore <i>truststore_path</i> | Specifies the path and file name of the trust store file. The default is \$CMUHOME/externalauth/IDMB/conf/system/truststore.                                                                                                                                   |
| -storepass <i>password</i>       | Specifies the password of the truststore file.                                                                                                                                                                                                                 |
| -file <i>certificate</i>         | Specifies the location of the public certificate to import. If you used <i>Create a Key/Certificate for Sterling Connect:Enterprise</i> on page 197, this certificate is located in \$CMUHOME/spd/cert.txt.<br>Do not use your private key or key/certificate. |

Following is an example:

```
$ keytool -import -keystore $CMUHOME/externalauth/IDMB/conf/system/truststore
-storepass mypassword -file $CMUHOME/spd/cert.txt
```

2. Details of the certificate are displayed and you are prompted with the following:

```
Trust this certificate?
```

Type **yes** and press **Enter** to trust the certificate.

---

## Start Sterling Connect:Enterprise and the External Authentication Service

Use the following procedure to start Sterling Connect:Enterprise and the External Authentication Service:

1. Start Sterling Connect:Enterprise using **ceustartup**.
2. Start the external authentication service type the following command and press **Enter**.

```
cmurefresh -h passphrase
```

where *passphrase* is the passphrase you changed in step 1 on page 193.

## Create and Identify a Security Definition for the External Authentication Service

Use the following procedure to create a security definition to define the Sterling Connect:Enterprise side of the secure communications to the external authentication service.

1. Using the Site Administration user interface, click **Define Security**.
2. Set the following parameters:

| Parameter              | Value                                                                                                                                                                                                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security protocol name | A name for the security definition.                                                                                                                                                                                     |
| Security               | Required                                                                                                                                                                                                                |
| Cipher Suites          | Select cipher suites in order of preference from 1-9.                                                                                                                                                                   |
| Authentication         | ServerClient                                                                                                                                                                                                            |
| SSL server CCC policy  | Disallowed                                                                                                                                                                                                              |
| SSL client CCC policy  | Disallowed                                                                                                                                                                                                              |
| Verify common name     | False                                                                                                                                                                                                                   |
| Root certificate file  | The certificate file that identifies the external authentication service. This is the certificate exported in <i>Export the External Authentication Service Certificate to Sterling Connect:Enterprise</i> on page 196. |
| Key certificate file   | Sterling Connect:Enterprise key/certificate file.                                                                                                                                                                       |

3. Click **Save**.
4. Click **Define Configuration**.
5. Select the configuration definition you are using and click **Edit**.
6. Set the following parameters:

| Parameter          | Description                                                                                                                                                        | Valid Value                                                                                                                                                                 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External auth      | Specifies whether external authentication or Sterling Connect:Enterprise authentication is used.<br>Specify Yes or RSD to use the external authentication service. | No = Default; use Sterling Connect:Enterprise authentication.<br>Yes = Use external authentication.<br>RSD = Authentication method is determined by the account definition. |
| External auth port | Specifies the port that the external authentication service listens on.                                                                                            | Any port between 1-65535. The default is 61365.                                                                                                                             |

| Parameter                 | Description                                                                                                                                                                                                                                                                        | Valid Value                                       |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| External auth secure port | Specifies the SSL port that the external authentication service listens on.                                                                                                                                                                                                        | Any port between 1-65535. The default is 61366.   |
| Control port              | Specifies the port that Sterling Connect:Enterprise uses to send the passphrase to the external authentication service.                                                                                                                                                            | Any port between 1-65535. The default is 61367.   |
| External auth resource    | Specifies the name of a default server access definition or server group on the external authentication service. During the initial configuration, it is normal for this field to be blank. This does not prevent you from communicating with the external authentication service. | Any valid access definition or server group name. |
| External auth host        | Specifies the host that the external authentication service runs on. Use this if you are connecting to an external authentication service that is installed separate from the Sterling Connect:Enterprise instance you are configuring.                                            | Any valid host name. The default is CMUHOST.      |
| External auth path        | Specifies the fully qualified path name of the executable for the external authentication service. You cannot specify both External auth host and External auth path.                                                                                                              | Any valid path.                                   |
| External auth SPD         | Specify the Security Definition you created in step 2 on page 199.                                                                                                                                                                                                                 | Any valid security definition.                    |

7. Click **Save**.

## Enable the Secure Access Acceptor

Use the following procedure to define the external authentication side of the secure connection from Sterling Connect:Enterprise.

1. Using the Site Administration user interface, click **Define Access Acceptor**.
2. Select **Secure** from the list and click **Edit**.
3. Set the following parameters:

| Parameter        | Value  |
|------------------|--------|
| Acceptor enabled | Enable |



| Parameter         | Value                                                              |
|-------------------|--------------------------------------------------------------------|
| Port              | Port number of the External Auth Secure Port in step 6 on page 199 |
| Secure connection | Enable                                                             |

4. Verify that the remaining values on this screen are correct:

| Parameter                   | Value                                                                                                                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time out                    | Any value.                                                                                                                                                                                        |
| Protocol                    | Secure protocol used to connect. The default is system.                                                                                                                                           |
| External Auth Keycert alias | Alias name of the key/certificate of the external authentication service. This is the certificate created in <i>Create a Key/Certificate for the External Authentication Service</i> on page 195. |
| Keystore file               | Path and file name of the keystore file. The default is <code>\$CMUHOME/externalauth/IDMB/conf/system/keystore</code> .                                                                           |
| Keystore password           | Password to the keystore.                                                                                                                                                                         |
| Truststore file             | Path and file name of the truststore file. The default is <code>\$CMUHOME/externalauth/IDMB/conf/system/truststore</code> .                                                                       |
| Truststore password         | Password to the keystore.                                                                                                                                                                         |

5. Click **Next**. A summary screen is displayed.
6. Verify the information in the summary screen and click **Save**.

---

## Restart and Verify the Secure Connection

Use the following procedure to activate the changes made and verify that you have a secure connection.

1. Shutdown Sterling Connect:Enterprise using **ceushutdown**.
2. Start Sterling Connect:Enterprise using **ceustartup**.
3. Start the external authentication service using **cmurefresh -h externalauthpassphrase**. Where `externalauthpassphrase` is the password you changed to in step 1 on page 193.
4. Using the Site Administration user interface, click **Define Access Acceptor**.
5. If Secure is available in the LDAP acceptor name list, the secure connection between Sterling Connect:Enterprise and the external authentication service is successful.
6. Click **Edit** to verify the parameters.

---

## Define the Server Access Definition

After you have established your secure connection between Sterling Connect:Enterprise and the external authentication service, define the communication and authentication methods between the external authentication service and your LDAP server. Refer to *Define Access* and *Define Access Group* in the Site Administration User Interface. Instructions can be found in the *Site Administration User Interface Help*.

---

## Disable the Nonsecure Port (Optional)

After you establish an SSL connection between the external authentication service and Sterling Connect:Enterprise, Sterling Connect:Enterprise no longer sends requests to the nonsecure port, although the external authentication service is still listening on the nonsecure port. Use the following procedure to disable the nonsecure port. Do not perform this procedure until you are certain that your SSL connection is working properly. If your SSL connection is not working properly and you disable your nonsecure port, you will need to perform all of the procedures in this chapter again.

1. Click **Define Access Acceptor** on the navigation panel.
2. Select **NonSecure** from the list and click **Edit**.
3. Disable **Acceptor enabled**.
4. Click **Save**.

---

## Changing Your Keystore Password After Your Key/Certificate Is Added (Optional)

If you need to change the password of the keystore after the external authentication service is running with a secure connection to Sterling Connect:Enterprise, use the procedure detailed in step 5 on page 193. But because the password for the keystore must be the same as the password for the external authentication key/certificate that resides in the keystore, you must also change the password of the key/certificate. Use the following command:

```
keytool -keypasswd -alias keycertalias -keypass keycertpassword -new
newkeycertpassword
```

The following table describes the command elements:

| Element | Description                  |
|---------|------------------------------|
| keytool | Invokes the keytool utility. |

## Changing Your Keystore Password After Your Key/Certificate Is Added (Optional)

| <b>Element</b>         | <b>Description</b>                                                                      |
|------------------------|-----------------------------------------------------------------------------------------|
| -storepasswd           | Instructs keytool to change the password of a certificate.                              |
| -alias                 | Instructs keytool that the text that follows is the alias of the certificate to change. |
| <i>certalias</i>       | The alias name of the certificate that you want to change.                              |
| -keypass               | Instructs keytool that the text that follows is current password of the certificate.    |
| <i>certpassword</i>    | The current password of the certificate.                                                |
| -new                   | Instructs keytool that the text that follows is current password of the certificate.    |
| -storepass             | Instructs keytool that the text that follows is the new password for the certificate.   |
| <i>newcertpassword</i> | New password of the certificate.                                                        |

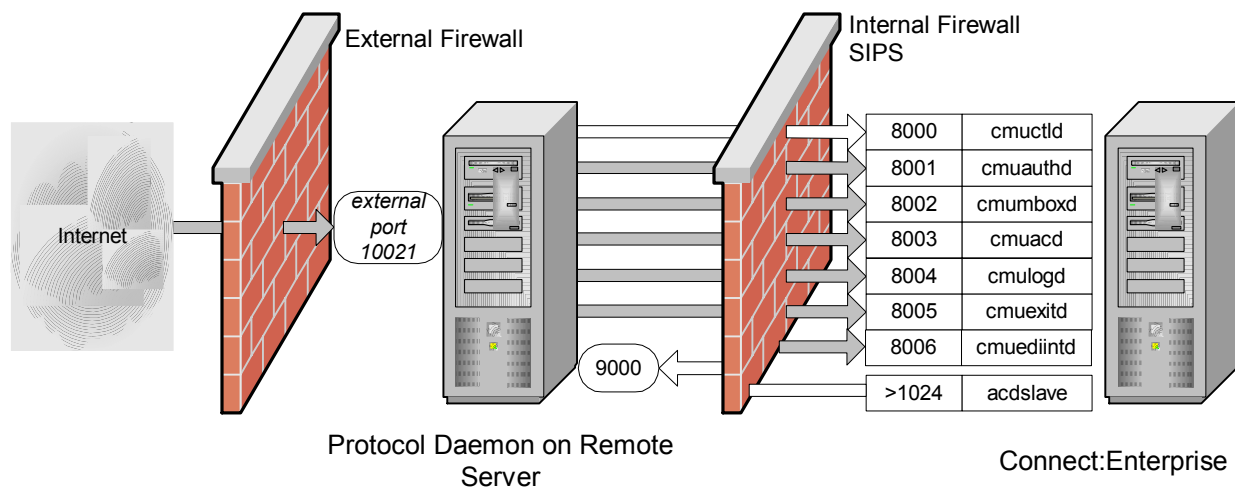


## Running Protocol Daemons on Remote Servers

Sterling Connect:Enterprise allows you to run a protocol daemon on a different server than your Sterling Connect:Enterprise server is running on. This allows you, for example, to run your FTP daemon or SSH daemon in the DMZ and still have through communication to Sterling Connect:Enterprise. This chapter describes how to set up your remote daemons.

### Firewall Considerations

To run a protocol daemon on a remote server, you must have the proper communication ports available through the firewall. The following diagram shows how the protocol daemon on the remote server communicates both externally, and with Sterling Connect:Enterprise. The port numbers identified are examples. Work with your firewall administrator to make sure the network path between the remote computer and the internal Sterling Connect:Enterprise server complies with your network security policy.



When Sterling Connect:Enterprise is started, the protocol daemon on the remote server uses an ephemeral port to connect to the control daemon (cmuctrld, port 8000) on Sterling Connect:Enterprise. The control daemon passes to the remote protocol daemon the ports that the other daemons are listening for SIPS on (ports 8001-8006). You can encrypt this communication using SIPS encryption (refer to *Configuring for Sterling Connect:Enterprise Components Running on Different Computers* on page 238).

Grey arrows indicate communication traffic when the external protocol daemon is performing a file transfer. The protocol daemon sends protocol messages to remote trading partners and SIPS messages to the Sterling Connect:Enterprise core daemons. If necessary, child daemons are forked.

White arrows indicate connections that must stay available as long as the product is running. Keep alive polls are sent every 5 minutes to avoid firewall timeouts.

---

## Installing the Remote Daemons

Currently, Sterling Connect:Enterprise allows you to run the following daemons from a remote server:

- ◆ FTP (cmuftp)
- ◆ SSH (cmusshftpd)
- ◆ HTTP (cmuhttpd) for AS2
- ◆ Admin (cmuadmind) for WebDAV

Use the following procedure to install the necessary files on the remote server.

1. Decide what daemon you want to run on a remote server.
2. Decide what server you want to run the daemon on.
3. Move the Sterling Connect:Enterprise installation media to the server you want to run the remote daemon on.
4. Run the installation script to install the remote daemons. Refer to *Installing Sterling Connect:Enterprise Remote Daemons* on page 39.
5. Refer to *Encrypting Internal Product Communications* on page 237 for information on encrypting communications between Sterling Connect:Enterprise and the remote daemons.

---

## Configuring SSL for AS2

If you install the HTTP daemon as a remote daemon and you want to require remote clients to connect using SSL, you will need to add SSL information to the port definition on the remote daemon. Use the following procedure.

1. Place a key certificate in a directory on the server where the remote daemon is running.
2. Navigate to the following directory on the remote server:

`$(CMUHOME)/as2`

3. Open AS2-Configuration.xml. Following is a sample:

```
<?xml version="1.0" encoding="UTF-8"?>
<AS2Configuration
xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.
11 AS2Configuration.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11">
    <ConfigurationName>RemoteHTTP</ConfigurationName>
    <ListeningPort>8880</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <DeadLetterMailbox>deadmbx</DeadLetterMailbox>
  </Port>
</AS2Configuration>
```

The values for the xml elements in this file were set during the installation.

4. Add the xml element to define the SSL parameters as show in bold in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<AS2Configuration
xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.
11 AS2Configuration.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11">
    <ConfigurationName>RemoteHTTP</ConfigurationName>
    <ListeningPort>8880</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <DeadLetterMailbox>deadmbx</DeadLetterMailbox>
    <SSLServer>
    </SSLServer>
  </Port>
</AS2Configuration>
```

5. To the SSLServer element, indicate the location of the key certificate you specified in step 1 on page 206 as shown in bold in the following example:

```

<?xml version="1.0" encoding="UTF-8"?>
<AS2Configuration
xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.
11 AS2Configuration.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11">
    <ConfigurationName>RemoteHTTP</ConfigurationName>
    <ListeningPort>8880</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <DeadLetterMailbox>deadmbx</DeadLetterMailbox>
    <SSLServer>
      <KeyCert>path and file name of key certificate</KeyCert>
    </SSLServer>
  </Port>
</AS2Configuration>

```

6. To the SSLServer element, indicate the cipher suites you will use. You have two options:

- ◆ Specify a cipher strength as **Strong** or **All**. The cipher suites are select based on strength. The xml to specify cipher strength is in bold in the following example:

```

<?xml version="1.0" encoding="UTF-8"?>
<AS2Configuration
xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.
11 AS2Configuration.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11">
    <ConfigurationName>RemoteHTTP</ConfigurationName>
    <ListeningPort>8880</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <DeadLetterMailbox>deadmbx</DeadLetterMailbox>
    <SSLServer>
      <KeyCert>path and file name of key certificate</KeyCert>
      <AcceptableCipherSuites>
        <CipherSuiteStrength>Strong</CipherSuiteStrength>
      </AcceptableCipherSuites>
    </SSLServer>
  </Port>
</AS2Configuration>

```

- ◆ Specify one or more cipher suites. The xml to specify one or more ciphers is in bold in the following example:



```

<?xml version="1.0" encoding="UTF-8"?>
<AS2Configuration
xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.
11 AS2Configuration.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/AS2/Configuration/v0.11">
    <ConfigurationName>RemoteHTTP</ConfigurationName>
    <ListeningPort>8880</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <DeadLetterMailbox>deadmbx</DeadLetterMailbox>
    <SSLServer>
      <KeyCert>path and file name of key certificate</KeyCert>
      <AcceptableCipherSuites>
        <CipherSuites>
          <CipherSuite
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">DHE_DS
S_EXPORT1024 / DES_CBC / SHA</CipherSuite>
          <CipherSuite
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">DHE_DS
S_EXPORT1024 / RC4_56 / SHA</CipherSuite>
        </CipherSuites>
      </AcceptableCipherSuites>
    </SSLServer>
  </Port>
</AS2Configuration>

```

You can specify any of the following cipher suites:

- DH\_anon\_EXPORT / DES40\_CBC / SHA
- DH\_anon\_EXPORT / RC4\_40 / MD5
- DH\_anon / DES\_CBC / SHA
- DH\_anon / RC4\_128 / MD5
- RSA\_EXPORT1024 / DES\_CBC / SHA
- RSA\_EXPORT1024 / RC4\_56 / SHA
- RSA / 3DES\_EDE\_CBC / SHA
- RSA / DES\_CBC / SHA
- RSA / NULL / MD5
- RSA / NULL / SHA
- RSA / RC4\_128 / MD5
- RSA / RC4\_128 / SHA
- DHE\_RSA / 3DES\_EDE\_CBC / SHA
- DHE\_RSA / DES\_CBC / SHA
- DHE\_RSA\_EXPORT / DES40\_CBC / SHA

7. If you plan to run AS2 with the remote HTTP daemon for auto-connects, a copy of the AS2-Configuration.xml must be placed in the \$CMUHOME/as2 directory on the remote daemon install. For each contract, this copy must include (at a minimum), the contract name, AS2 identifiers, and remote URL and SSL settings. Also, this file must include any HTTP proxy definitions. This AS2-Configuration.xml is not configurable through the Site Administration User Interface and must be synchronized manually when changes affecting any of the above are made to the AS-2 Configuration.xml on the core server.

---

## Configuring SSL for WebDAV

If you install the Admin daemon (for WebDAV) as a remote daemon and you want to require remote clients to connect using SSL, you will need to add SSL information to the port definition on the remote daemon. Use the following procedure.

1. Place a key certificate in a directory on the server where the remote daemon is running.
2. If you will perform client authentication, place the trusted certificates file on the server where the remote daemon is running.
3. Navigate to the following directory on the remote server:

```
$CMUHOME/cpd/admin/
```

4. Open Admind.xml. Following is a sample:

```
<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 Admind.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
    <ConfigurationName>RemoteAdmin</ConfigurationName>
    <ListeningPort>8881</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <AuthenticationType>BASIC</AuthenticationType>
    <SessionTimeout>5</SessionTimeout>
  </Port>
</ADMINDConfiguration>
```

The values for the xml elements in this file were set during the installation.

5. Add the xml element to define the SSL parameters as show in bold in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 Admind.xsd">
<Port xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
  <ConfigurationName>RemoteAdmin</ConfigurationName>
  <ListeningPort>8881</ListeningPort>
  <InternetIdentity>
    <FQDN>hostorIP</FQDN>
  </InternetIdentity>
  <AuthenticationType>BASIC</AuthenticationType>
  <SessionTimeout>5</SessionTimeout>
  <SSLServer>
  </SSLServer>
</Port>
</ADMINDConfiguration>
```

6. To the SSLServer element, indicate the location of the key certificate you specified in step 1 on page 206 as shown in bold in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 Admind.xsd">
<Port xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
  <ConfigurationName>RemoteAdmin</ConfigurationName>
  <ListeningPort>8881</ListeningPort>
  <InternetIdentity>
    <FQDN>hostorIP</FQDN>
  </InternetIdentity>
  <AuthenticationType>BASIC</AuthenticationType>
  <SessionTimeout>5</SessionTimeout>
  <SSLServer>
    <KeyCert>path and file name of key certificate</KeyCert>
  </SSLServer>
</Port>
</ADMINDConfiguration>
```

7. To the SSLServer element, indicate the type of authentication to perform, as shown in bold in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 Admind.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
    <ConfigurationName>RemoteAdmin</ConfigurationName>
    <ListeningPort>8881</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <AuthenticationType>BASIC</AuthenticationType>
    <SessionTimeout>5</SessionTimeout>
    <SSLServer>
      <KeyCert>path and file name of key certificate</KeyCert>
      <SSLType>SERVERCLIENT</SSLType>
    </SSLServer>
  </Port>
</ADMINDConfiguration>
```

You can specify either of the following:

- ◆ SERVERONLY = Client connections authenticate the Sterling Connect:Enterprise for UNIX server using the key certificate file.
  - ◆ SERVERCLIENT = Client connections authenticate the Sterling Connect:Enterprise for UNIX server using the Key certificate file. The Sterling Connect:Enterprise for UNIX server authenticates the client using the Root certificate file.
8. If you specified SERVERCLIENT in step 7, add to the SSLServer element the location of the trusted certificate file to use for client authentication as shown in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 Admind.xsd">
  <Port xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
    <ConfigurationName>RemoteAdmin</ConfigurationName>
    <ListeningPort>8881</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <AuthenticationType>BASIC</AuthenticationType>
    <SessionTimeout>5</SessionTimeout>
    <SSLServer>
      <KeyCert>path and file name of key certificate</KeyCert>
      <SSLType>SERVERCLIENT</SSLType>
      <TrustedCertificates>path and file name of trusted certificates file
    </TrustedCertificates>
    </SSLServer>
  </Port>
</ADMINDConfiguration>
```

9. To the SSLServer element, indicate the cipher suites you will use. You have two options:
- ◆ Specify a cipher strength as **Strong** or **All**. This will automatically select the cipher suites to use based on strength. The xml to specify cipher strength is in bold in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 AdminD.xsd">
<Port xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
  <ConfigurationName>RemoteAdmin</ConfigurationName>
  <ListeningPort>8881</ListeningPort>
  <InternetIdentity>
    <FQDN>hostorIP</FQDN>
  </InternetIdentity>
  <AuthenticationType>BASIC</AuthenticationType>
  <SessionTimeout>5</SessionTimeout>
  <SSLServer>
    <KeyCert>path and file name of key certificate</KeyCert>
    <SSLType>SERVERCLIENT</SSLType>
    <TrustedCertificates>path and file name of trusted certificates file
    </TrustedCertificates>
    <AcceptableCipherSuites>
      <CipherSuiteStrength>Strong</CipherSuiteStrength>
    </AcceptableCipherSuites>
  </SSLServer>
</Port>
</ADMINDConfiguration>
```

- ◆ Specify one or more cipher suites. The xml to specify one or more ciphers is in bold in the following example:

```

<?xml version="1.0" encoding="UTF-8"?>
<ADMINDConfiguration
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/
v0.11 Admind.xsd">
  <Port
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">
    <ConfigurationName>RemoteAdmin</ConfigurationName>
    <ListeningPort>8881</ListeningPort>
    <InternetIdentity>
      <FQDN>hostorIP</FQDN>
    </InternetIdentity>
    <AuthenticationType>BASIC</AuthenticationType>
    <SessionTimeout>5</SessionTimeout>
    <SSLServer>
      <KeyCert>path and file name of key certificate</KeyCert>
      <SSLType>SERVERCLIENT</SSLType>
      <TrustedCertificates>path and file name of trusted certificates file
      </TrustedCertificates>
      <AcceptableCipherSuites>
        <CipherSuites>
          <CipherSuite
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">TLS_RSA_WITH_RC4_
128_MD5</CipherSuite>
          <CipherSuite
xmlns="http://www.sterlingcommerce.com/ceu/ADMIND/Configuration/v0.11">TLS_RSA_WITH_RC4_
128_SHA</CipherSuite>
        </CipherSuites>
      </AcceptableCipherSuites>
    </SSLServer>
  </Port>
</ADMINDConfiguration>

```

You can specify any of the following cipher suites:

- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_DES\_CBC\_SHA
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- TLS\_RSA\_WITH\_NULL\_MD5
- TLS\_RSA\_WITH\_NULL\_SHA
- TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5
- TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

---

# Configuring High Availability

Sterling Connect:Enterprise supports the failover capabilities of IBM high-availability cluster multi-processing (HACMP), Sun Cluster, and Hewlett-Packard MC/Service Guard high-availability software using bisynchronous and FTP protocols. This chapter provides information specific to how Sterling Connect:Enterprise handles those failover capabilities.

---

## Installing Sterling Connect:Enterprise High-Availability Scripts

The Sterling Connect:Enterprise high-availability core scripts are automatically installed in the `$CMUHOME/etc/ha` default location. The platform-specific sample scripts are installed in `$CMUHOME/etc/ha/arch`, where *arch* = solaris, hpux, or aix.

These scripts are installed with every Sterling Connect:Enterprise for UNIX installation. In order to take advantage of this capability, you must customize the scripts for each local installation.

See the Sun, IBM, and HP Web sites for high-availability support:

- ◆ Solaris documentation Web site: <http://docs.sun.com/>
- ◆ HP documentation Web site: <http://www.docs.hp.com/hpux/onlinedocs/>
- ◆ IBM documentation Web site: <http://www-1.ibm.com/servers/eserver/pseries/library/>

## Customizing Sterling Connect:Enterprise for the High-Availability Feature

If you decide to use the high availability feature after you install Sterling Connect:Enterprise, you must customize Sterling Connect:Enterprise manually using the following steps:

1. If you created a password for Sterling Connect:Enterprise and the system prompts for it at startup, add the `CMUPASWD` environment variable to the `rcfiles` `kshrc`, `cshrc`, and `profile` to enable Sterling Connect:Enterprise to start without prompting for a password. The minimum requirement is that the password must be in `$CMUHOME/etc/profile`.

---

**Caution:** The high-availability Package Manager cannot start if Sterling Connect:Enterprise prompts for a password.

---

2. Change the CMUHOST value in the rcfiles to the shared host name of the cluster, not the host name of an individual computer. For example, you have two computers named *part* and *some* in a cluster named *all*. Set the CMUHOST value to *all* to ensure that either *part* or *some* can service any inbound connections addressed to *all*.
3. If you installed the File Agent, \$CMUHOME/etc/fileagt.cfg must also reference the shared host name of the cluster. Edit the fileagt.cfg file in \$CMUHOME/etc/ and change cmu= to the shared host name.
4. Log in as the Sterling Connect:Enterprise user, change directories to \$CMUHOME/etc, and run ceinstall.

The following prompt is displayed:

```
The following directory (called the destination directory):
/host/users/user01/ceunix21
was detected to be the location of Sterling Connect:Enterprise for UNIX.

Is this correct? (Y|n)
```

The script continues and verifies that all files are in the correct location. CMUHOME, CMUSER, and CMUPORT are replaced with appropriate values throughout the high-availability configuration files, and the script then displays the following message:

```
=====
=
IBM(R) Sterling Connect:Enterprise(R) for UNIX
Version 1.3 High-Availability Package Installation Procedure

The Sterling Connect:Enterprise for UNIX High-Availability Package
Installation Procedure is complete. You must now register the
High-Availability package with the Package Manager. Please
reference the appropriate instructions in the Sterling Connect:Enterprise for
UNIX High-Availability Package Installation Guide.
=====
=
Press Enter...
```

When you press Enter, the script exits. If the script is being run from another script such as ceinstall, it returns to its calling script.

## Configuring Protocol Daemons for the High-Availability Feature

If the protocol daemons are being operated on a computer separate from the cluster and the core Sterling Connect:Enterprise daemons on the cluster are configured for the high-availability feature, the protocol daemons must also be configured to use the high-availability feature to ensure that the computer running the remote protocol daemons fails over if it loses the connection with the control daemon. Configuring the protocol daemons to use the high-availability feature also enables them to be restarted and does not impede the operation of Sterling Connect:Enterprise.



## Sterling Connect:Enterprise Core High-Availability Scripts

This section describes the core scripts that Sterling Connect:Enterprise uses in a high-availability environment. By default, all core high-availability scripts are located in \$CMUHOME/etc/ha. The following table describes the functions of the high-availability core scripts and the configuration required to use Sterling Connect:Enterprise for UNIX in a high-availability environment.

| Script       | Description                                                                                                                                                                                                                                                                                                                                 | Required Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| proc_mon.cfg | Used by all core scripts to start, stop, and monitor Sterling Connect:Enterprise processes and maintain a functioning system. It is the single point of process configuration for the Sterling Connect:Enterprise high-availability scripts.                                                                                                | <p>A sample proc_mon_cfg is installed and configured by cehainstall. The cmuftp daemon is enabled by default. To use the Bisync daemons, Async daemon, or the File Agent, edit this file and uncomment any or all of the following daemons: ceufileagt, cmuasyd, cmubscda, and cmubscdc.</p> <p>To use the Site Administration user interface, add the cmusvid daemon (Service Interface daemon) and add the <code>-p portno</code> parameter, where <code>portno</code> specifies the port that the cmusvid daemon will monitor for inter-process communication. Refer to the <i>cmusvid—Service Interface Daemon</i> on page 82 for more information on the <code>-p</code> parameter.</p> |
| ce_ha_start  | <p>Starts the daemons listed in the proc_mon.cfg file. It must be run as root. This script can use the value of the first column in the proc_mon.cfg file as an argument. For example, typing <code>ce_ha_start_cmuftp</code> starts cmuftp by itself.</p> <p>This feature is used by ce_ha_probe to restart specific protocol daemons.</p> | <p>No configuration is necessary.</p> <p>Note: See the <i>Using Core Scripts without Implementing High Availability</i> on page 220 for information on using this script in an environment that does not implement the high-availability feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ce_ha_stop   | Stops the daemons listed in the proc_mon.cfg file. It must be run as root and takes no arguments. This script is intended to be run by the high-availability Package Manager.                                                                                                                                                               | <p>No configuration is necessary.</p> <p>Note: See the <i>Using Core Scripts without Implementing High Availability</i> on page 220 for information on using the script in an environment that does not implement the high-availability feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Script      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Required Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ce_ha_probe | <p>Performs the following functions:</p> <ul style="list-style-type: none"> <li>Monitors the core daemons configured in the <code>proc_mon.cfg</code> file using the <b>ps</b> command. Upon failure of any of the core daemons, the probe script finishes active Sterling Connect:Enterprise processes and then fails over to the standby computer.</li> <li>Monitors any uncommented protocol daemons defined in the <code>proc_mon.cfg</code> file using the <b>ps</b> command. Upon failure of a protocol daemon, the probe script attempts to restart the daemon the number of times specified in <code>proto.retries</code> for that daemon. If the protocol cannot be restarted, the probe script stops Sterling Connect:Enterprise using <code>ce_svc_stop</code>, finishes active Sterling Connect:Enterprise processes, and fails over to the standby computer.</li> </ul> | <p>No configuration is necessary on the HP-UX platform.</p> <p>For AIX and Solaris platforms:</p> <ol style="list-style-type: none"> <li>Open the <code>\$CMUHOME/etc/ha/ce_ha_probe</code> file using <code>vi</code> or a similar text editor. The first portion of the file is marked as the user-modifiable section.</li> <li>Edit the <code>NOTIFY_FUNCTION</code> parameter to enable email notification of a failover. You can uncomment the mail line to cause an email notification to be sent each time a failover occurs.</li> </ol> |

### Syntax and Parameters for the `proc_mon.cfg` Script

This following example contains the syntax of the `proc_mon.cfg` file, which must be typed on one line.

```
process_name:process_owner:core|proto.retries:startup_command_line
```

The values are defined in the following table:

| Value                      | Description                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>process_name</code>  | Specifies the process name that returns when the <b>ps -edaf</b> command is issued. Indicates whether a given process is active or inactive.                              |
| <code>process_owner</code> | Specifies the process owner for the processes identified by the <b>ps -edaf</b> command. The default is the UNIX user who installed and runs Sterling Connect:Enterprise. |

| Value                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| core proto.retries   | <p>Determines what to restart in the event of a failover.</p> <p>coreSets value to core daemon. (cmuctld, cmuexitd, cmuacd, cmulogd, and cmumboxd). A core daemon failure results in Sterling Connect:Enterprise failing over.</p> <p>protoSets value of proto.retries. A protocol daemon failure results in only the protocol being restarted. A system failover occurs when the number of retries exceeds the value defined in proto.retries.</p> <p><b>Note:</b> For bisync protocol on all platforms, set proto.retries to proto.0 to initiate an immediate failover if the bisync parent process fails and the child process continues running. If proto.retries is not set to 0, inbound transfers are handled properly, but new outbound transfers fail and the autoconnect is removed from the queue.</p> <p><b>Note:</b> For FTP on the AIX platform, set proto.retries to proto.0 to initiate an immediate failover when the process started by the parent cmuftp daemon is stopped and the Package Manager cannot restart the parent process because its child process continues running.</p> |
| startup_command_line | Specifies the exact startup command needed to start the process. The ce_ha_start script has the Sterling Connect:Enterprise bin directory in its path, so only the executable file name is required.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Following is an sample proc\_mon.cfg script:

```

cmuctld:uid1:core:cmuctld -P 22110 -l 99 -d /tmp/ctld.out &
cmuauthd:uid1:core:cmuauthd -H 127.0.0.1 -P 22110 &
cmumboxd:uid1:core:cmumboxd -H 127.0.0.1 -P 22110 &
cmuacd:uid1:core:cmuacd -H 127.0.0.1 -P 22110 &
cmulogd:uid1:core:cmulogd -H 127.0.0.1 -P 22110 &
cmuexitd:uid1:core:cmuexitd -H 127.0.0.1 -P 22110 &
# Note that the bisync daemons must be set to proto.0 in order to properly
# clean up the 3780 processes that hang around when they die prematurely.
#cmubscda:uid1:proto.0:cmubscda -H 127.0.0.1 -P 22110 &
#cmubscdc:uid1:proto.0:cmubscdc -H 127.0.0.1 -P 22110 &
#cmuasyd:uid1:proto.2:cmuasyd -H 127.0.0.1 -P 22110 &
cmuftp daemon:uid1:proto.2:cmuftp daemon -H 127.0.0.1 -P 22110 &
cmusvid:uid1:proto.2:cmusvid -H 127.0.0.1 -P 22110 -p 22150 -l 99 -d /tmp/svid.out&
#ceufileagt:uid1:proto.2:${CMUHOME}/etc/cefastartup.sh &

```

## Arguments for the ce\_ha\_probe Script

The ce\_ha\_probe script accepts the following arguments:

| Argument | Description                                                                                                         |
|----------|---------------------------------------------------------------------------------------------------------------------|
| -s       | Stands for single invocation. Marks failed daemons, restarts any daemons that need to be restarted, and then exits. |

| Argument          | Description                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -c                | Stands for check only. Lists any daemons that are missing and then exits as follows:<br>0 = All daemons are accounted for.<br>1 = Some daemons are missing; does not stop the system or perform a failover.                          |
| -v                | Stands for verbose. Prints a list of specific actions taken by the probe script.                                                                                                                                                     |
| no argument given | The script runs in a loop, testing the status of Sterling Connect:Enterprise every 30 seconds. It performs any necessary restarts. Upon detection of a failover condition, the script issues a FAILOVER message to stdout and exits. |

## Using Core Scripts without Implementing High Availability

The `ce_ha_start` and `ce_ha_stop` scripts can be used in an environment that does not implement high availability. You must edit the user-modifiable portions of the `ce_ha_probe` script using `vi` or a similar UNIX text editor.

1. Edit the `SINGLE_MACH_MONITOR` variable in the `ce_ha_probe` script. By default, the Package Manager transfers Sterling Connect:Enterprise operations to the designated standby computer. This option is not available without the high availability feature.
2. Change the `SINGLE_MACH_MONITOR` variable from `FALSE` to `TRUE` to restart Sterling Connect:Enterprise when the script is being used to monitor processes without High Availability. A restart on the same system results instead of a fail over to another high availability system node.
3. Use the `ce_ha_start` script to start Sterling Connect:Enterprise, then start the `ce_ha_probe` script to monitor and restart Sterling Connect:Enterprise. Both scripts must be run as the root superuser.

## Sun Solaris High-Availability Implementation

The Sun Solaris high-availability scripts are divided into service-stop and service-start scripts and service monitor-stop and monitor-start scripts. The service scripts start and stop Sterling Connect:Enterprise, whereas the service monitor scripts start a monitor daemon that monitors the function of Sterling Connect:Enterprise. The monitor daemon restarts Sterling Connect:Enterprise if a failure occurs, and if the restart fails, it stops Sterling Connect:Enterprise and fails over to the standby host.

Note these important characteristics of the Sun implementation of high availability:

- ◆ Sterling Connect:Enterprise must be started and stopped using the `scswitch` command in the Package Manager.
- ◆ If the package fails over from computer A to computer B, and then back to computer A again too quickly, the Package Manager stops Sterling Connect:Enterprise on both computers, marks them both as *offline*, and does not attempt to restart them until the start command (`/usr/cluster/bin/scswitch -Z -g ce-harg`) is issued on one of the computers.

- ◆ When you configure your high-availability package, ensure that the shared host name and IP address belong to the ce-harg resource group so that when Sterling Connect:Enterprise operations fail over to the standby host, the shared host name and IP address are transferred also. Placing the shared host name and IP address in the ce-harg resource group ensures that the hosts and resources remain synchronized during failover and Sterling Connect:Enterprise operations continue uninterrupted.

The following table lists each Sun-specific high-availability script and provides a brief description of its function. These scripts are located in \$CMUHOME/etc/ha/solaris by default.

| Script           | Description                                                                                                                                                                                                                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ce_monitor_start | Starts the probe script.                                                                                                                                                                                                                                                                                                                                            |
| ce_monitor_stop  | Stops the probe script, usually in preparation for failover.                                                                                                                                                                                                                                                                                                        |
| ce_monitor_check | Checks the current status of the probe script to ensure it is still running.                                                                                                                                                                                                                                                                                        |
| ce_svc_start     | Starts Sterling Connect:Enterprise.<br>0 = Start is successful.<br>1 = Start failed.                                                                                                                                                                                                                                                                                |
| ce_svc_stop      | Stops Sterling Connect:Enterprise cleanly.<br>0 = Stop is successful, or Sterling Connect:Enterprise was not running.<br>Nonzero return = Stop failed. (The script was unable to stop Sterling Connect:Enterprise.)<br>Note: If a shutdown cannot be done cleanly, the stop script forcibly stops all Sterling Connect:Enterprise processes as cleanly as possible. |
| ce_svc_probe     | Polls the activity of Sterling Connect:Enterprise repeatedly while it is running. This script calls ce_ha_probe -s, and fails over based on the criteria set in the core script ce_ha_probe.                                                                                                                                                                        |
| ce_update        | Used by the Package Manager at registration.                                                                                                                                                                                                                                                                                                                        |
| ce_validate      | Used by the Package Manager at registration.                                                                                                                                                                                                                                                                                                                        |
| SCI.ce           | This Resource Type Registration file contains configuration entries that point the Package Manager to the other scripts in the \$CMUHOME/etc/ha.solaris directory.                                                                                                                                                                                                  |

## Resource Type Registration File

The Sun-specific scripts are identified for the cluster manager in the Resource Type Registration (RTR) file, SCI.ce. More information about the RTR file is available on the Sun documentation Web site.

## Configuring the ce\_svc\_start and ce\_svc\_stop Scripts

Edit the SCI.ce configuration file and specify RT\_BASEDIR= *full path name of Solaris base directory*, for example, RT\_BASEDIR=/global/cluster/ceunix/etc/ha/solaris.

---

**Note:** You cannot substitute environment variables such as \$CMUHOME in this parameter. You must use the full path name of the directory.

---

## Configuring the ce\_svc\_probe Script

If you are using a terminal server with a daemon that must start and stop during failovers, modify the `NXCDCMD` and `NXCDFILE` variables to identify the terminal server. The script checks for the existence of the variable value before it tries to run a command, so it is permissible to leave the variables blank.

## Registering Sterling Connect:Enterprise with the Sun Package Manager

1. To register Sterling Connect:Enterprise to work properly with the Sun Package Manager, create a new package type using the `SCI.ce` configuration file located in `$CMUHOME/etc/ha/solaris`, as follows:

```
cd $CMUHOME/etc/ha/solaris
/usr/cluster/bin/scrgadm -a -t SCI.ce -f ./SCI.ce
```

2. Add the failover resource group as follows:

```
/usr/cluster/bin/scrgadm -a -g ce-harg
```

3. Create the resource for the resource type as root. Type the following command on one line. It must not be on two lines as it appears in the following example.

```
/usr/cluster/bin/scrgadm -a -j ce-hars -g ce-harg -t SCI.ce -y
Port_list=8000/tcp,10021/tcp -x Confdir=$CMUHOME/etc/ha
```

4. Replace the `Port_list=` values of `8000/tcp` and `10021/tcp` with the values you specified in your installation of Sterling Connect:Enterprise.
5. Verify the registration as follows:

```
/usr/cluster/bin/scrgadm -p
/usr/cluster/bin/scstat -p
```

Ensure the `ce-hars` resource is offline on both cluster hosts.

6. Start Sterling Connect:Enterprise by typing:

```
/usr/cluster/bin/scswitch -Z -g ce-harg
```

7. Verify the `ce-hars` resource group is online on the current host by typing:

```
/usr/cluster/bin/scstat -p
```

## Commands Used with the Sun Solaris High-Availability Implementation

The following table lists some frequently used commands that are specific to the Sun implementation of high availability.

| Command                                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/usr/cluster/bin/scswitch -R -h <i>hostname</i> -g ce-harg</code>                                                                                                                                                                                                                                                                        | Restarts the system.                                                                                                                                                                                                                                |
| <code>/usr/cluster/bin/scswitch -z -g ce-harg -h <i>newhost</i></code>                                                                                                                                                                                                                                                                         | Switches from one host to another specified by <i>newhost</i> .                                                                                                                                                                                     |
| <code>/usr/cluster/bin/scswitch -c -h <i>hostname</i> -j ce-hars -f STOP_FAILED</code>                                                                                                                                                                                                                                                         | Clears error flags. In this example, you received a STOP_FAILED when Sterling Connect:Enterprise could not cleanly shut down.                                                                                                                       |
| <code>/usr/cluster/bin/scswitch -n -j ce-hars</code><br><code>/usr/cluster/bin/scswitch -z -g ce-harg -h ""</code><br><code>/usr/cluster/bin/scswitch -u -g ce-harg</code><br><code>/usr/cluster/bin/scrgadm -r -j ce-hars</code><br><code>/usr/cluster/bin/scrgadm -r -g ce-harg</code><br><code>/usr/cluster/bin/scrgadm -r -t SCl.ce</code> | Sequence of commands deletes resource and group definitions and unregisters Sterling Connect:Enterprise from the high-availability Package Manager configuration files.<br><br>NOTE: The commands must be issued in the order they are listed here. |
| <code>/usr/local/cluster/bin/scswitch -S -h <i>hostname</i> shutdown -g0 -y -i6</code>                                                                                                                                                                                                                                                         | Reboots a cluster node cleanly.                                                                                                                                                                                                                     |

## Hewlett-Packard High-Availability Implementation

Sterling Connect:Enterprise for UNIX is fully integrated with the Hewlett-Packard MC/ServiceGuard high-availability software. Sterling Connect:Enterprise can be monitored and controlled by MC/ServiceGuard, which provides high-availability capability in a mission-critical environment. You can configure the monitoring level based on your specific needs and how you configure Sterling Connect:Enterprise.

**Note:** MC/ServiceGuard does not use any of the core Sterling Connect:Enterprise high-availability scripts, but it does use the `proc_mon.cfg` configuration file. See the *Sterling Connect:Enterprise Core High-Availability Scripts* on page 217 and the *Syntax and Parameters for the `proc_mon.cfg` Script* on page 218 for specific configuration information.

### High-Availability Scripts

The following table lists the HP-UX high-availability scripts and describes their function. These scripts are located in `$CMUHOME/etc/ha/hpux` by default.

| Script      | Description                                                                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| control.sh  | Master control script for MC/ServiceGuard in Sterling Connect:Enterprise. Initializes, terminates, starts, and stops the Sterling Connect:Enterprise package and all associated resources. Modify this file for your specific volume information and your installation of MC/ServiceGuard. |
| ce_services | Starts and monitors Sterling Connect:Enterprise processes. It is called from control.sh.                                                                                                                                                                                                   |
| ce_svc_stop | Stops Sterling Connect:Enterprise.                                                                                                                                                                                                                                                         |

## Configuration Files

Two configuration files are used with Sterling Connect:Enterprise. The package configuration file for Sterling Connect:Enterprise is the ce.ascii file, also located in \$CMUHOME/etc/ha/hpux. Modify the contents of the ce.ascii file as specified in the following table:

| Item                      | Value                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------|
| NODE_NAME                 | hp1<br>(Based on cluster; this parameter must be modified to reflect local settings.)        |
| NODE_NAME                 | hp2<br>(Based on cluster; this parameter must be modified to reflect local settings.)        |
| RUN_SCRIPT                | /etc/cmcluster/ce/control.sh<br>(Ensure that your scripts are located in /etc/cmcluster/ce.) |
| HALT_SCRIPT               | /etc/cmcluster/ce/control.sh<br>(Ensure that your scripts are located in /etc/cmcluster/ce.) |
| SERVICE_NAME              | ceu_core                                                                                     |
| SERVICE_FAIL_FAST_ENABLED | NO                                                                                           |
| SERVICE_HALT_TIMEOUT      | 300                                                                                          |
| SERVICE_NAME              | eu_bscd                                                                                      |
| SERVICE_FAIL_FAST_ENABLED | NO                                                                                           |
| SERVICE_HALT_TIMEOUT      | 300                                                                                          |
| SERVICE_NAME              | ceu_asyd                                                                                     |
| SERVICE_FAIL_FAST_ENABLED | NO                                                                                           |



| Item                                   | Value                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------------|
| SERVICE_HALT_TIMEOUT                   | 300                                                                                                     |
| SERVICE_NAME                           | ceu_ftp                                                                                                 |
| SERVICE_FAIL_FAST_ENABLED              | NO                                                                                                      |
| SERVICE_HALT_TIMEOUT                   | 300                                                                                                     |
| SERVICE_NAME                           | ceu_fileagt                                                                                             |
| SERVICE_FAIL_FAST_ENABLED              | NO                                                                                                      |
| SERVICE_HALT_TIMEOUT                   | 300                                                                                                     |
| Fill in any other services needed here |                                                                                                         |
| SUBNET                                 | 10.20.40.0<br>(Ensure that this parameter is configured appropriately based on your local environment.) |

The cluster.ascii configuration file is an MC/ServiceGuard configuration file that is specific to the Package Manager and is not shipped with Sterling Connect:Enterprise. The following sample cluster.ascii file provides you with configuration data about volumes and packages to assist you in

understanding the dependencies of the Hewlett-Packard high-availability script files. See the Hewlett-Packard high-availability documentation for additional information.

```
# *****
# ***** HIGH AVAILABILITY CLUSTER CONFIGURATION FILE *****
# ***** For complete details about cluster parameters and how to *****
# ***** set them, consult the ServiceGuard manual. *****
# *****

# Enter a name for this cluster. This name will be used to identify the
# cluster when viewing or manipulating it.

CLUSTER_NAMEcluster1

# Cluster Lock Parameters
#
# The cluster lock is used as a tie-breaker for situations
# in which a running cluster fails, and then two equal-sized
# sub-clusters are both trying to form a new cluster. The
# cluster lock is configured using a lock disk.
#
# Consider the following when configuring a cluster:
# for a two-node cluster, you must use a cluster lock; for
# a cluster of three or four nodes, a cluster lock is
# strongly recommended.

# Lock Disk Parameters. Use the FIRST_CLUSTER_LOCK_VG and
# FIRST_CLUSTER_LOCK_PV parameters to define a lock disk.
# The FIRST_CLUSTER_LOCK_VG is the LVM volume group that
# holds the cluster lock. This volume group should not be
# used by any other cluster as a cluster lock device.

FIRST_CLUSTER_LOCK_VG/dev/ce

# Definition of nodes in the cluster.
# Repeat node definitions as necessary for additional nodes.

NODE_NAMEhp1
  NETWORK_INTERFACElan0
  HEARTBEAT_IP10.20.40.80
  FIRST_CLUSTER_LOCK_PV/dev/dsk/c0t0d0
# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE/dev/tty0p0

# Warning: There are no standby network interfaces for lan0.

# Cluster Timing Parameters (microseconds).
```

```

# The NODE_TIMEOUT parameter defaults to 2000000 (2 seconds).
# This default setting yields the fastest cluster reformatations.
# However, the use of the default value increases the potential
# for spurious reformatations due to momentary system hangs or
# network load spikes.
# For a significant portion of installations, a setting of
# 5000000 to 8000000 (5 to 8 seconds) is more appropriate.
# The maximum value recommended for NODE_TIMEOUT is 30000000
# (30 seconds).

HEARTBEAT_INTERVAL1000000
NODE_TIMEOUT2000000

# Configuration/Reconfiguration Timing Parameters (microseconds).

AUTO_START_TIMEOUT6000000000
NETWORK_POLLING_INTERVAL2000000

# Package Configuration Parameters.
# Enter the maximum number of packages which will be configured in the cluster.
# You can not add packages beyond this limit.
# This parameter is required.
MAX_CONFIGURED_PACKAGES9

# List of cluster aware LVM Volume Groups. These volume groups will
# be used by package applications via the vgchange -a e command.
# Neither CVM or VxVM Disk Groups should be used here.
# For example:
# VOLUME_GROUP/dev/vgdatabase
# VOLUME_GROUP/dev/vg02

VOLUME_GROUP/dev/ce

```

## Configuring Sterling Connect:Enterprise for the HP High-Availability Environment

The following procedures outline the installation process and configuration changes required to use Sterling Connect:Enterprise in the Hewlett-Packard high-availability environment. Refer to the *IBM Sterling Connect:Enterprise for UNIX Installation Guide* for complete, detailed instructions for installing Sterling Connect:Enterprise. The nodes used to illustrate this cluster environment are hp1, the primary node, and hp2, the standby node.

1. Create a volume group to put the shared logical volumes on, such as /dev/ce.
2. Create a logical volume on the new volume group with a mount point, such as /dev/ce/ce, mounted under /ce.
3. Mount the shared logical volume.
4. Install Sterling Connect:Enterprise as detailed in the *IBM Sterling Connect:Enterprise for UNIX Installation and Administration Guide*.
5. Set up and configure Sterling Connect:Enterprise, connecting to the system IP.

---

**Note:** Verify the product works as expected BEFORE moving to the MC/ServiceGuard integration phase.

---

6. Unmount the shared directories.
7. On hp1, deactivate the volume group, mark the volume group as a member of the high-availability cluster, and export volume group /dev/ce/ to a map file:

```
vgchange -a n /dev/ce
vgchange -c y /dev/ce
vgexport -m ce.map -s -p -v /dev/ce
```

8. Copy the ce.map file to hp2, the standby node, using FTP.

```
ftp hp2
put /tmp/ce.map /tmp/ce.map
quit
```

9. Use Telnet to connect to hp2.
10. On hp2, create the /dev/ce directory and control file (group) with the same major and minor numbers.
11. Import the volume group information:

```
vgimport -m ce.map -s -v /dev/ce
```

12. Mount /ce to confirm the import was successful.

## Setting Up Sterling Connect:Enterprise for a Two-Node MC/ServiceGuard Cluster

When the shared file system can be mounted on both systems, set up and configure the MC/ServiceGuard scripts for Sterling Connect:Enterprise. The hp1 system is the primary node in this two-node MC/ServiceGuard cluster; the standby node in this cluster is hp2.

### Setting Up Sterling Connect:Enterprise on the hp1 Node

1. Establish the volume group /dev/ce on a disk array dual-ported to node hp1 and node hp2.
2. Establish the following logical volume and mount the VxFS file systems under the respective mount points:

```
/dev/ce/ce
/ce
```

3. Ensure that the fully qualified domain name is used for both the physical node name and the floating package IP for the Sterling Connect:Enterprise package. Also ensure that the fully qualified domain name is typed before any aliases and before the short host name in /etc/hosts, in DNS, or in NIS/NIS+.
4. Install Sterling Connect:Enterprise as detailed in the *IBM Sterling Connect:Enterprise for UNIX Installation and Administration Guide*.

## Setting Up the hp2 Node

Before work is started on the standby node, the shared disks must be exported by the primary node and imported by the standby node.

1. From hp1, export volume group /dev/ce to a map file, deactivate the volume group, and transfer the map file to hp2 using FTP:

```
vgexport -m /tmp/ce.map -p -v -s /dev/ce
vgchange -a n /dev/ce
ftp hp2
put /tmp/ce.map /tmp/ce.map
quit
```

2. On hp2, create volume group /dev/ce, import the volume group information, and activate the volume group. Ensure that the major number of the group file is the same as it is on hp1.

```
mkdir /dev/ce
mknod /dev/ce/group c 64 0x010000
vgimport -m /tmp/ce.map -v -s /dev/ce
vgchange -a y /dev/ce
```

3. Mount all relevant file systems:

```
mkdir /ce
/etc/mount /dev/ce/ce /ce
```

## Configuring the MC/ServiceGuard Cluster

The following steps describe creating and using the MC/ServiceGuard scripts.

1. Create the ASCII cluster template file, cluster.ascii:

```
cmquerycl -v -C /etc/cmcluster/cluster.ascii -n hp1 -n hp2
```

2. Modify the cluster.ascii template file with environment-specific information and verify the cluster configuration:

```
cmcheckconf -v -C /etc/cmcluster/cluster.ascii
```

3. Create the cluster by applying the configuration file. This step creates the cmclconfig binary file and automatically distributes it among the nodes defined in the cluster.

```
cmapplyconf -v -C /etc/cmcluster/cluster.ascii
```

4. Start the cluster, check the cluster status, and test the cluster halt function:

```
cmruncl -v -n hp1 -n hp2
cmviewcl -v
cmhaltcl -f -v
cmruncl -n hp1 -n hp2
```

## Configuring the ServiceGuard Package on a Single Node

The following steps configure a ServiceGuard package on hp1, the primary node.

1. Create the ce package configuration file and tailor it to your test environment. Do not include the second node at this stage.

```
cd /etc/cmcluster
mkdir ce
cmmakepkg -p ce.ascii# Edit ce.ascii
```

2. Create the ce package control script and tailor it to your test environment. Do not include application startup/shutdown, service monitoring, or relocatable IP address at this stage.

```
cd ce
cmmakepkg -s control.sh
```

3. Stop the cluster and verify and distribute the binary configuration files.

```
cmhaltcl -f -v
cmapplyconf -v -C /etc/cmcluster/cluster.ascii -P /etc/cmcluster/ce/ce.ascii
```

4. Test the cluster and package startup:
  - a. Stop Sterling Connect:Enterprise.
  - b. Unmount all logical volumes on /dev/ce.
  - c. Deactivate the volume group.
  - d. Copy the ce\_services, ce\_svc\_stop, control.sh, and ce.ascii scripts to /etc/cmcluster/ce.
  - e. Type the following command:

```
cmruncl          # Start cluster and package
cmviewcl -v     # Check that package has started
```

5. Edit the ce.cnt1 file and assign the dynamic IP address of the ce package.

```
cmhaltpkg ce
vi control.sh          # Edit to add package IP
cmrunpkg -v ce        # Start Ce Package
cmviewcl -v           # Check package has started and clients
```

6. Enable switching to a local standby LAN card.

```
vi ce.ascii          # Net switching enabled = YES
cmapplyconf -v -C /etc/cmcluster/cluster.ascii -P ce.ascii
cmhaltcl -f -v
cmruncl -v
```

## Adding the Second Node to the ServiceGuard Package

Use the following steps to add hp2 to the ServiceGuard single-node package.

1. Edit the package control file to enable Sterling Connect:Enterprise to switch to a second node.

```
vi ce.conf # add NODE_NAME hp2
cmapplyconf -v -C /etc/cmcluster/cluster.ascii -P ce/ce.ascii
cmhaltcl -f -v
cmruncl -v
```

2. Test package switch to hp2 and back to hp1.

```
cmhaltpkg ce
cmrunpkg -n hp2 ce # Run package on hp2 and
# run ce and check application
cmmodpkg -e ce # Enable package switching
cmhaltpkg ce
cmrunpkg -n hp1 ce # Run package on hp1 and test
# ce runs here
cmmodpkg -e ce
```

The ce package is running using the system host name instead of the package IP.

## Sample Output of the cmviewcl Command

The following sample output shows the result when you issue the cmviewcl -v command with the ce package running on the hp1 node.

```
CLUSTER      STATUS
cluster1    up

NODE         STATUS      STATE
hp1         up          running

Network_Parameters:
INTERFACE    STATUS      PATH        NAME
PRIMARY     up         8/8/1/0     lan1
PRIMARY     up         8/8/2/0     lan2
STANDBY     up         8/16/6      lan5

PACKAGE      STATUS      STATE        PKG_SWITCH  NODE
ce           up          running     enabled     hp1

Policy_Parameters:
POLICY_NAME   CONFIGURED_VALUE
Failover     configured_node
Failback     manual
```

```

Script_Parameters:
ITEM          STATUS   MAX_RESTARTS  RESTARTS  NAME
Service      up         3             0         ce
Subnet       up                192.6.77.0

Node_Switching_Parameters:
NODE_TYPE     STATUS   SWITCHING  NAME
Primary      up       enabled    hp1      (current)
Alternate    up       enabled    hp2

NODE          STATUS   STATE
hp2          up       running

Network_Parameters:
INTERFACE     STATUS   PATH        NAME
PRIMARY      up       8/8/1/0     lan1
STANDBY      up       8/16/6      lan5
PRIMARY      up       8/8/2/0     lan2

```

## Commands Used with the Hewlett-Packard High-Availability Implementation

The following table lists some frequently used commands that are specific to Hewlett-Packard systems.

| Command                                    | Purpose                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| cmrunpkg ce                                | Starts the ce package.                                                                                                                              |
| cmhaltpkg ce                               | Stops the ce package.                                                                                                                               |
| cmruncl                                    | Starts the cluster.                                                                                                                                 |
| cmhaltcl                                   | Stops the cluster when no packages are running.                                                                                                     |
| cmhaltcl -f                                | Stops the cluster when packages are running.                                                                                                        |
| cmmodpkg -e <i>packagename</i>             | Enables a package to fail over.                                                                                                                     |
| cmmodpkg -e -n <i>nodename packagename</i> | Enables the specified package to run on the node that failed. Use after a failover to enable the package to run on the node that previously failed. |
| cmviewcl                                   | View status of cluster and packages.                                                                                                                |
| cmhaltpkg <i>packagename</i>               | Halts the specified package.                                                                                                                        |

**Caution:** In the event of a failure, all Sterling Connect:Enterprise processes being held are restarted when the ce package restarts, including any Sterling Connect:Enterprise processes intentionally held by Operator.



## AIX High-Availability Implementation

The AIX high-availability package is configured by default to start the service monitor daemon. The monitor daemon starts, monitors, and stops Sterling Connect:Enterprise as necessary. If the service monitor stops, the AIX high-availability manager fails over to the standby computer.

The following table lists the high-availability scripts for AIX and provides a brief description of their function. These scripts are located in \$CMUHOME/etc/ha/aix by default.

| Script      | Description                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CE_start.sh | Starts the CE_probe.sh script.                                                                                                                                                                                                                                                                                                                                                                                              |
| CE_stop.sh  | Stops the CE_probe.sh script.<br>0 = Stop successful, or Sterling Connect:Enterprise is not running.<br>Nonzero = Stop failed. (The script was unable to stop Sterling Connect:Enterprise.)<br>NOTE: If a shutdown cannot be done cleanly, the stop script forcibly shuts down all Sterling Connect:Enterprise processes as cleanly as possible.                                                                            |
| CE_probe.sh | Repeatedly polls the activity of Sterling Connect:Enterprise while it is running. If the system is not active, the probe script attempts to restart it one time and then instructs the AIX manager to fail over to the standby node. If the attempt to restart succeeds, or if it fails but Sterling Connect:Enterprise can be restarted, the script returns a value of 0 (zero). Otherwise, it returns a value of nonzero. |

### Configuring the Sterling Connect:Enterprise AIX High-Availability Scripts

Use the following steps to configure the CE\_start.sh script.

1. Open the CE\_start.sh script using a text editor and modify the following variables:

```
export CMUHOME=/shrfs1/sci/ceunix
export PATH=/usr/es/sbin/cluster/utilities:$PATH
export NCXDCMD="/etc/ncxd -p771 /dev/sa3 192.168.1.16"
export NCXDFILE=/etc/ncxd
```

2. Replace the value for CMUHOME with the global Sterling Connect:Enterprise home directory available to all computers in the cluster.
3. Modify PATH to contain the cluster utilities directory.
4. If you are using a terminal server with a daemon that must start and stop during failovers, modify the NCXDCMD and NCXDFILE variables (in this example the terminal server is the Digi Etherlite **ncxd**). The script checks for the existence of the variable value before it tries to run a command, so it is permissible to leave the variables blank.

Use the following steps to configure the CE\_stop.sh script.

1. Open the `CE_stop.sh` script using a text editor and modify the following variables:

```
export CMUHOME=/shrfs1/sci/ceunix
export NCXDPSSTRING=ncxd
```

2. Replace the value for `CMUHOME` with the global Sterling Connect:Enterprise home directory available to all computers in the cluster.
3. Replace the value for `NCXDPSSTRING` (default of `ncxd`) with your terminal server software, or if you are not using a terminal server, set this value to a process name that will never be returned by the `ps -edaf` command (such as `no_term_server`).

Use the following steps to configure the `CE_probe.sh` script.

1. Open the Sterling Connect:Enterprise\_`probe.sh` script using a text editor and modify the following variables:

```
export CMUHOME=/shrfs1/sci/ceunix
export SHAREDHOSTIP="192.168.1.3"
export PATH=/usr/es/sbin/cluster/utilities:$PATH
export NCXDCMD="/etc/ncxd -p771 /dev/sa3 192.168.1.16"
export NCXDFILE=/etc/ncxd
```

2. Replace the value for `CMUHOME` with the global Sterling Connect:Enterprise home directory available to all computers in the cluster.
3. Modify the value for `SHAREDHOSTIP` to contain the global IP address for the failover cluster. This permits the probe script to detect whether the failover cluster is running on the current primary host.
4. Modify the `PATH` variable to contain the cluster utilities directory.
5. If you are using a terminal server with a daemon that must start and stop during failovers (in this example the terminal server is the Digi Etherlite `ncxd`), perform the following steps:
  - a. Modify the `NCXDCMD` and `NCXDFILE` variables to identify the terminal server. The `CE_probe.sh` script checks for the existence of the variable value before it tries to run a command, so it is permissible to leave the variables blank.
  - b. Remove the terminal server daemon from the `/etc/inittab` file and from the system rc scripts. You must ensure that the daemon is configured correctly in the `NCXD*` variables in the `CE_start.sh`, `CE_stop.sh`, and `CE_probe.sh` scripts.

---

**Note:** To prevent multiple nodes from connecting to the terminal server at the same time, the terminal server daemon must be started by the `CE_start.sh` script and stopped by the `CE_stop.sh` script.

---

## Registering Sterling Connect:Enterprise with the AIX Package Manager

The following procedures illustrate how to register Sterling Connect:Enterprise with the AIX high-availability Package Manager, which allows the Package Manager to start, monitor, and stop Sterling Connect:Enterprise. If the service monitor stops, the AIX high-availability manager fails over to the standby computer.

Registering Sterling Connect:Enterprise with the AIX high-availability Package Manager consists of the following tasks: adding a resource group, adding an application server, changing or showing resources or attributes for a resource group, and synchronizing the cluster. You accomplish these tasks using the HACMP menus and panels, where you type or select values for the fields.

## Adding a Resource Group

To add a resource group:

1. From the UNIX command prompt, start the HACMP application by typing:

```
smit hacmp
```

This command displays the HACMP menu.

2. Select Cluster Configuration.
3. From the Cluster Configuration menu, select Cluster Resources and press Enter.
4. From the Cluster Resources menu, select Define Resource Groups and press Enter.
5. From the Define Resource Groups menu, select Add a Resource Group and press Enter.
  - a. In the Resource Group Name field, type **ce**.
  - b. In the Node Relationship field, select **cascading**.
  - c. Ensure that the participating node names are correct.
  - d. Press Enter to save these values. After you save these values, the HACMP application returns you to the UNIX command prompt.

## Adding an Application Server

To add an application server:

1. From the UNIX command prompt, type **smit hacmp**.
2. Select Cluster Configuration and press Enter.
3. From the Cluster Configuration menu, select Cluster Resources and press Enter.
4. From the Cluster Resources menu, select Define Applications Servers and press Enter.
5. From the Define Applications Servers menu, Select Add an Application Server and press Enter.
  - a. In the Server Name field, type the server names, for example, **ce\_01** and **ce\_02**.
  - b. In the Start Script field specify the full path to **CE\_start.sh**.
  - c. In the Stop Script field, specify the full path to **CE\_stop.sh**.
  - d. Press Enter to save these values.

## Changing or Showing Resources or Attributes for a Resource Group

To change or display resources or attributes of a resource group:

1. From the UNIX command prompt, type **smit hacmp**.
2. Select Cluster Configuration and press Enter.
3. From the Cluster Configuration menu, select Cluster Resources and press Enter.
4. From the Cluster Resources menu, select Change/Show Resources for a Resource Group and press Enter.
  - a. Select either `ce_01` or `ce_02`.
  - b. Ensure that the information in the fields is correct for both groups and that the service IP labels correspond to the application server instances.

## Synchronizing Cluster Resources

To synchronize the cluster:

1. From the UNIX command prompt, type **smit hacmp**.
2. Select Cluster Configuration and press Enter.
3. From the Cluster Configuration menu, select Cluster Resources and press Enter.
4. From the Cluster Resources menu, select Synchronize Cluster Resources and press Enter.

If you need additional information, see your AIX HACMP documentation for specific procedures.

---

# Encrypting Internal Product Communications

Sterling Connect:Enterprise for UNIX components such as core daemons, protocol daemons, offline commands, and user-written API programs use messages to communicate to each other. These messages can contain sensitive data such as user passwords and repository batch data.

Use the information in this chapter to enable Sterling Connect:Enterprise to encrypt these internal communication messages using a secure, strong encryption algorithm. This feature is only available with Secure FTP.

---

## Enabling Message Encryption

Perform the following steps to enable internal message encryption:

1. With Sterling Connect:Enterprise for UNIX running, specify **Enable SIPS encryption=Yes** in the Define Configuration function of the Site Administration user interface.
2. Stop Sterling Connect:Enterprise for UNIX. Refer to Chapter 5, *Starting and Stopping Sterling Connect:Enterprise* for more information.
3. Create the encryption key file using the following command:

```
cmusipskey -n hostname -p portnumber
```

where *hostname* specifies the name of the host where the Control daemon is running and *portnumber* specifies the port number the Control daemon is monitoring.

This command creates a base 64-encoded encryption key in the following file: `$CMUHOME/keys/sipskeys`. Sterling Connect:Enterprise uses the encryption key to create session keys. A new session key is created each time Sterling Connect:Enterprise is started. Sterling Connect:Enterprise uses the session key to encrypt messages.

**Note:** If a previous `$CMUHOME/keys/sipskeys` file already exists, this command renames the existing `sipskeys` file to `$CMUHOME/keys/sipskeys.old.yyyymmdd.hhmmss`.

4. Start Sterling Connect:Enterprise for UNIX. Refer to Chapter 5, *Starting and Stopping Sterling Connect:Enterprise* for more information.

---

## Configuring for Sterling Connect:Enterprise Components Running on Different Computers

If you are running a Sterling Connect:Enterprise protocol daemon, API program, or offline command from a remote computer (any computer other than the computer Sterling Connect:Enterprise is running on), use the following procedure:

1. Place a copy of the sipskeys file generated in *Enabling Message Encryption* on page 237 in a directory on the computer that is running the Sterling Connect:Enterprise component.
2. Set the CEUSIPSKEYLOCATION environment variable on the remote computer to identify the full path of the sipskeys file from step 1. Following is an example:

```
export CEUSIPSKEYLOCATION=/data/users/user01/sipskeys
```

---

## Configuring for Components Connecting to Multiple Sterling Connect:Enterprise Instances

If you are running a Sterling Connect:Enterprise Sterling B2B Integrator adapter, API program, or offline command on a remote computer (any computer other than the computer Sterling Connect:Enterprise is running on) that connects to multiple instances of Sterling Connect:Enterprise, use the following procedure:

1. Collect the sipskeys files for each instance of Sterling Connect:Enterprise that the remote computer communicates with.
2. Combine the contents of the sipskeys files collected in step 1 to a single sipskeys file. Following is a sample key file for a remote computer that communicates with three instances of Sterling Connect:Enterprise:

```
ceserver01 9976 o1FF9Bsp8pdBQSo+Aj6nUpvegA8d
ceserver02 9976 /S5Hcc1pNHpijdKnh1ipvFnzjBRo
ceserver03 9976 XsBb1hT3/IqH3DRQhLhTE82h1B/r
```

3. Set the CEUSIPSKEYLOCATION environment variable on the remote computer to identify the full path of the sipskeys file from step 1. Following is an example:

```
export CEUSIPSKEYLOCATION=/data/users/user01/sipskeys
```

---

# Error Messages

This chapter covers the following topics:

- ◆ Sterling Connect:Enterprise Error Codes
- ◆ Sterling Connect:Enterprise Error Codes—These errors are generated by the Command Line Utilities or by the Sterling Connect:Enterprise daemons. The utilities write these errors to `stderr` and the daemons write them to the file name specified when each daemon was started (using the `-d` and `-l` switches).
- ◆ Sterling Connect:Enterprise API Error Codes—These errors are generated by the Command Line Utilities and user-written programs that use the Sterling Connect:Enterprise API. The utilities write these errors to `stderr`.
- ◆ Sterling Connect:Enterprise Auto Connect Status Codes—These status codes are displayed by the **cmureport** utility.
- ◆ Sterling Connect:Enterprise Remote Connect Status Codes—These status codes are displayed by the **cmureport** utility.
- ◆ Sterling Connect:Enterprise Utilities Exit Codes—These error codes are generated when Sterling Connect:Enterprise utilities exit.
- ◆ Authorization Log Message IDs—These error messages are displayed in the authentication log file.

## Sterling Connect:Enterprise Error Codes

The following is the numerical listing of Sterling Connect:Enterprise error codes:

| Decimal | Hex     | Error Text                        | Description                                                                                                                                                                                                                                             | Action                                                                                                                                               |
|---------|---------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERROR   | ERROR   | disk full, shutting down...       | In the course of writing logging information to the log file, a check is made to see if the disk is full. If this error is encountered, this message is displayed. Upon displaying this message, Sterling Connect:Enterprise is automatically shutdown. | Determine what is causing the disk to be full and make adjustments. Ensure that the limits set for the Sterling Connect:Enterprise log are adequate. |
| 524     | 0x020C  | CMURC_SIPS_VERSION_ERROR          | Received the wrong version SIPS message.                                                                                                                                                                                                                | Verify that all headers are compatible versions.                                                                                                     |
| 525     | 0x0020D | CMURC_SIPS_DECRYPTI<br>ON_FAILED  | Encrypted message received, but not decrypted.                                                                                                                                                                                                          | Contact IBM support.                                                                                                                                 |
| 526     | 0x020E  | CMURC_SIPS_ENCRYPTI<br>ON_FAILED  | SIPS encryption failed.                                                                                                                                                                                                                                 | Contact IBM support.                                                                                                                                 |
| 527     | 0x020F  | CMURC_SIPS_MSG_ENC<br>RYPTED      | Encrypted message was received, but a plain message was expected.                                                                                                                                                                                       | Contact IBM support.                                                                                                                                 |
| 768     | 0x0300  | CMURC_SIPS_MSG_NOT<br>_ENCRYPTED  | Plain message received, but encrypted message was expected.                                                                                                                                                                                             | Contact IBM support.                                                                                                                                 |
| 769     | 0x0301  | CMURC_SIPS_KEYFILE_<br>ERROR      | Cannot access the SIPS key file.                                                                                                                                                                                                                        | Verify that a SIPS key file exists in the \$CMUHOME directory. You can create a new key using cmusipskey.                                            |
| 770     | 0x0302  | CMURC_SIPS_KEYFILE_<br>KEY_ERROR  | Key in SIPS key file is invalid.                                                                                                                                                                                                                        | Verify SIPS key in the key file. You can create a new key using cmusipskey.                                                                          |
| 771     | 0x0303  | CMURC_SIPS_ENCRYPT<br>_INIT_ERROR | Cannot initialize SIPS encryption.                                                                                                                                                                                                                      | Contact IBM support.                                                                                                                                 |
| 4096    | 0x1000  | CMURC_SIP_BADSTATE                | An unexpected message was received.                                                                                                                                                                                                                     | Generate a level 99 debug trace and contact IBM Customer Service.                                                                                    |
| 4097    | 0x1001  | CMURC_HOST_NOT_FO<br>UND          | IP address/host not found.'                                                                                                                                                                                                                             | Check the network connection, name server, or host file, then retry the connection.                                                                  |



| Decimal | Hex    | Error Text                 | Description                                                  | Action                                                                                                                             |
|---------|--------|----------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 4098    | 0x1002 | CMURC_LOGIN_FAILED         | Invalid user login request.                                  | Remote supplied an invalid username (remote ID) and/or password.                                                                   |
| 4112    | 0x1010 | CMURC_ARG_INVALID          | Invalid argument to a Sterling Connect:Enterprise operation. | Generate a level 99 debug trace and contact IBM Customer Service                                                                   |
| 4128    | 0x1020 | CMURC_DATABASE_NO MATCH    | No batches match selection criteria.                         | Investigate existence of batches matching the specified criteria.                                                                  |
| 4352    | 0x1100 | CMURC_EOF                  | End of file.                                                 | No action required.                                                                                                                |
| 4353    | 0x1101 | CMURC_TRUNC                | Record truncation occurred.                                  | Check the RECVBUFF size in the Bisync CPD file from the Site Administration Interface. It is too small for incoming data blocks.   |
| 4609    | 0x1201 | CMURC_RECEIVE_ERROR        | Error during receive operation.                              | Try reducing vulnerability to environmental conditions by reducing baud rate or block size from the Site Administration Interface. |
| 4610    | 0x1202 | CMURC_TRANSMIT_ERROR       | Error during transmit operation.                             | Try reducing vulnerability to environmental conditions by reducing baud rate or block size from the Site Administration Interface. |
| 4611    | 0x1203 | CMURC_BLOCK_SENT           | Block sent.                                                  | No action necessary.                                                                                                               |
| 4612    | 0x1204 | CMURC_IN_PROGRESS          | In progress.                                                 | No action necessary.                                                                                                               |
| 4613    | 0x1205 | CMURC_LOST_DTR             | Lost DTR during Bisync read/write.                           | Try reducing vulnerability to environmental conditions by reducing baud rate or block size from the Site Administration Interface. |
| 4864    | 0x1300 | CMURC_MBOXEXTRACT_IOERR    | File I/O error during extract operation.                     | Run file system consistency check (FSCK).                                                                                          |
| 4868    | 0x1301 | CMURC_MBOXEXTRACT_INDEXERR | I/O error on index file during extract operation.            | Run file system consistency check (FSCK).                                                                                          |

| Decimal | Hex    | Error Text                 | Description                      | Action                                                                                                                                                                                                                                                                                                    |
|---------|--------|----------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5120    | 0x1400 | CMURC_SHARED_ALLOC_FAILED  | Shared memory allocation failed. | This error is posted when a Sterling Connect:Enterprise daemon process exceeds the system imposed limit of the amount of shared memory that can be allocated by any one process. Increase the shared memory limit. If the error persists generate a level99 debug trace and contact IBM Customer Service. |
| 5121    | 0x1401 | CMURC_SHARED_ATTACH_FAILED | Shared memory attach failed.     | This error is posted when a Sterling Connect:Enterprise daemon process exceeds the system imposed limit of the number of shared memory segments that can be attached to a single process. Increase this limit. If the error persists, generate a level 99 debug trace and contact IBM Customer Service.   |
| 5122    | 0x1402 | CMURC_SHARED_DETACH_FAILED | Shared memory detach failed.     | Generate a level 99 debug trace and contact IBM Customer Service.                                                                                                                                                                                                                                         |
| 5123    | 0x1403 | CMURC_SHARED_REMOVE_FAILED | Shared memory remove failed.     | Generate a level 99 debug trace and contact IBM Customer Service.                                                                                                                                                                                                                                         |
| 5376    | 0x1500 | CMURC_SEM_CREATE_FAILED    | Semaphore creation failed.       | This error is posted when a Sterling Connect:Enterprise daemon process exceeds the system imposed limit of number of semaphores that can be created per process. Increase this limit. If the error persists, generate a level 99 debug trace and contact IBM Customer Service.                            |
| 5377    | 0x1501 | CMURC_SEM_REMOVE_FAILED    | Semaphore removal failed.        | Generate a level 99 debug trace and contact IBM Customer Service.                                                                                                                                                                                                                                         |
| 5378    | 0x1502 | CMURC_SEM_WAIT_FAILED      | Semaphore wait failed.           | Generate a level 99 debug trace and contact IBM Customer Service.                                                                                                                                                                                                                                         |

| Decimal | Hex    | Error Text               | Description                                                                                                                                                                    | Action                                                                                         |
|---------|--------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| 5379    | 0x1503 | CMURC_SEM_SIGNAL_FAILED  | Semaphore signal failed.                                                                                                                                                       | Generate a level 99 debug trace and contact IBM Customer Service.                              |
| 5632    | 0x1600 | CMURC_INVALID_FIELD_TYPE | Invalid field type passed to function.                                                                                                                                         | Generate a level 99 debug trace and contact IBM Customer Service.                              |
| 5888    | 0x1700 | CMURC_SESSION_ERROR      | Error during session request. One or more daemons are hung.                                                                                                                    | Issue <b>cmushutdown</b> at earliest convenience and restart.                                  |
| 6143    | 0x17FF | CMURC_EACCESS            | Access denied. The user is attempting an operation (like a <b>put</b> or <b>\$\$ADD</b> ) that violates the security permissions defined in <i>\$CMUHOME/med/mbxacl.conf</i> . | Update the <i>mbxacl.conf</i> file to give the user permission for the desired command.        |
| 6144    | 0x1800 | CMURC_MBOXADD_IO         | File I/O error during add operation.                                                                                                                                           | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6145    | 0x1801 | CMURC_MBOXADD_FILE       | I/O error opening file.                                                                                                                                                        | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6146    | 0x1802 | CMURC_MBOXADD_INDEXFILE  | I/O error opening index file.                                                                                                                                                  | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6147    | 0x1803 | CMURC_MBOXADD_INDEXIO    | I/O error writing index file.                                                                                                                                                  | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6148    | 0x1804 | CMURC_MBOXADD_STAT       | I/O error trying to STAT batch file.                                                                                                                                           | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6149    | 0x1805 | CMURC_MBOXADD_STATFS     | I/O error getting file system information.                                                                                                                                     | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6150    | 0x1806 | CMURC_MBOXADD_NOSPACE    | Out of disk space.                                                                                                                                                             | Re-attempt failing operation after freeing some disk space.                                    |

| Decimal | Hex    | Error Text                  | Description                                               | Action                                                                                         |
|---------|--------|-----------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------------------|
| 6151    | 0x1807 | CMURC_MBOXADD_SEEK          | Seek error during add operation.                          | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6152    | 0x1808 | CMURC_MBOXADD_MAXBATCHNO    | Attempt to exceed maximum batch number.                   | Increase the value of the MAXBATCHNO parameter in the \$CMUHOME/med/cmumbox.med file.          |
| 6153    | 0x1809 | CMURC_MBOXADD_MKDIR         | Error creating directory structure.                       | Verify path to UNIX mailbox is writable.                                                       |
| 6160    | 0x1810 | CMURC_MBOXADD_ADDBATCH      | Could not add batch to database.                          | Verify path to UNIX mailbox is writable.                                                       |
| 6165    | 0x1815 | CMURC_MBOXADD_NOLINK        | Invalid batch # during link operation.                    | Verify the batch number specified on <b>cmuadd</b> command and retry.                          |
| 6166    | 0x1816 | CMURC_MBOXADD_LINK          | Could not link to batch specified.                        | Verify existence of the file being referenced by the <b>cmuadd</b> command.                    |
| 6167    | 0x1817 | CMURC_MBOXADD_INDEXLINK     | Could not link to index file for batch.                   | Generate a level 99 debug trace and contact IBM Customer Service.                              |
| 6224    | 0x1850 | CMURC_MBOXEXTRACT_IO        | File I/O error during extract operation.                  | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6225    | 0x1851 | CMURC_MBOXEXTRACT_FILE      | I/O error on access/open of file.                         | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6226    | 0x1852 | CMURC_MBOXEXTRACT_INDEXFILE | I/O error on open of index file during extract operation. | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6227    | 0x1853 | CMURC_MBOXEXTRACT_INDEXIO   | I/O error reading index file.                             | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |
| 6228    | 0x1854 | CMURC_MBOXEXTRACT_SEEK      | Seek error while skipping control record.                 | Run file system consistency check (FSCK). If the problem continues, call IBM Customer Service. |

| Decimal | Hex    | Error Text                                 | Description                                                    | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|--------|--------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6229    | 0x1855 | CMURC_SYS_RESOURCE_ERROR                   | Too many files open or too many Processes.                     | This error is posted when a Sterling Connect:Enterprise daemon process exceeds the system imposed limit of number of processes it can fork or the number of files it can have opened. Increase the values for Configurable Kernel Parameters for Maximum Number of Open files, Maximum Number of Open Inodes, Maximum number of User Processes, or Maximum number of Processes. If the error persists generate a level 99 debug trace and contact IBM Customer Service. |
| 6400    | 0x1900 | CMURC_PROTOCOL_FAILED                      | Protocol process failed.                                       | Run a debug level 4 trace and look for a preceding error.                                                                                                                                                                                                                                                                                                                                                                                                               |
| 8192    | 0x2000 | CMURC_INVALID_BATCH_ID                     | Failed Security=Batch check ID                                 | Security=Batch is enabled and the remote ID of an inbound batch did not match an ID listed in the ValidIDList parameter of the MCD file. Doublecheck the <b>Security</b> and <b>Valid Mailbox ID list</b> parameters for <b>control.mcd</b> .                                                                                                                                                                                                                           |
| 8193    | 0x2001 | CMURC_SCRIPT_LOGIN_FAILED                  | Login from script failed.                                      | Send/Expect portion of the login script failed. Verify the script.                                                                                                                                                                                                                                                                                                                                                                                                      |
| 8194    | 0x2002 | CMURC_FAILED_TO_RECEIVE_TRANSLATION_BUFFER | Failed to receive user translation buffer from control daemon. | Generate a level 99 debug trace and contact IBM Customer Service.                                                                                                                                                                                                                                                                                                                                                                                                       |
| 12288   | 0x3000 | CMURC_BSC_ERROR_DIALING                    | Error during Bisync dial attempt.                              | Verify phone line is attached, modem is on, phone number is correct, etc.                                                                                                                                                                                                                                                                                                                                                                                               |
| 12289   | 0x3001 | CMURC_BSC_ERROR_INSTALL_STALL              | Error during install while dialing.                            | Generate a level 4 debug trace of the Bisync daemon and contact IBM Customer Service.                                                                                                                                                                                                                                                                                                                                                                                   |
| 12290   | 0x3002 | CMURC_BSC_ERROR_PORT_SETUP                 | Error during port setup while dialing.                         | Generate a level 4 debug trace of the Bisync daemon and contact IBM Customer Service.                                                                                                                                                                                                                                                                                                                                                                                   |

| Decimal | Hex    | Error Text                        | Description                                                                                                                                                                              | Action                                                                                                                                                                      |
|---------|--------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12291   | 0x3003 | CMURC_BSC_RT_NOTFO<br>UND         | Bisync runtime not found.                                                                                                                                                                | Verify the BSCRDIR environment variable is set and is correct.                                                                                                              |
| 12292   | 0x3004 | CMURC_BSC_RT_FAILED               | Bisync runtime failed to start.                                                                                                                                                          | Call IBM Customer Service.                                                                                                                                                  |
| 12295   | 0x3007 | CMURC_BSC_INTERRUPT<br>T          | Process interrupted for AC. An idle leased line was interrupted to begin a Auto Connect.                                                                                                 | No action necessary.                                                                                                                                                        |
| 12296   | 0x3008 | CMURC_BSC_GENERAL_<br>ERROR       | General error.                                                                                                                                                                           | Generate a level 4 debug trace on the Bisync daemon and look for additional errors.                                                                                         |
| 12297   | 0x3009 | CMURC_BSC_RVI_RECEI<br>VED        | Reverse interrupt received from remote.                                                                                                                                                  | No action necessary                                                                                                                                                         |
| 16384   | 0x4000 | CMURC_JES_LOGON_FA<br>ILED        | JES2 logon failed.                                                                                                                                                                       | Check contents of logon message for valid signon card against the LOGONMSG parameter in the RSD file for that remote.                                                       |
| 16385   | 0x4001 | CMURC_JES_LOGOFF_F<br>AILED       | JES2 logoff failed.                                                                                                                                                                      | Check contents of logoff message for valid signon card against the LOGOFFMSG parameter in the RSD file for that remote.                                                     |
| 28676   | 0x7004 | CMURC_<br>SSH_CONNECTION_LOS<br>T | Connection lost between the server and the client. If you are the client, the connection was lost on the server side. If you are the server, the connection was lost on the client side. | Attempt to reconnect. If the connection fails, contact the client or server administrator.                                                                                  |
| 28677   | 0x7005 | CMURC_<br>SSH_BAD_MESSAGE         | Bad arguments in message received; Invalid SFTP protocol parameters transmitted.                                                                                                         | Verify that you are using SFTP protocol parameters that are valid for SSHFTP. These are listed in the <i>IBM Sterling Connect:Enterprise for UNIX Remote User's Guide</i> . |
| 28678   | 0x7006 | CMURC_SSH_FAILURE                 | General error.                                                                                                                                                                           | View the trace file to identify the failure.                                                                                                                                |
| 28679   | 0x7007 | CMURC_<br>SSH_DIRECTORY           | Path does not specify a regular file/batch. The specified path does not identify a file or a Sterling Connect:Enterprise for UNIX batch.                                                 | Check the directory specified to ensure it identifies a file/batch.                                                                                                         |

| Decimal | Hex    | Error Text                 | Description                                                                                                      | Action                                                                                        |
|---------|--------|----------------------------|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| 28680   | 0x7008 | CMURC_SSH_PROTOCOL_VERSION | Incompatible protocol version expected but not received: server did not send client a valid SSH protocol version | Verify that you are using the SSH protocol supported by Sterling Connect:Enterprise for UNIX. |

## API Error Codes

The following is the numerical listing of the Sterling Connect:Enterprise API error codes. All API error codes are accompanied with CE error codes. Refer to the previous section.

| Decimal | Hex    | Error Text               | Description              | Action                                                                                                                         |
|---------|--------|--------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 0       | 0x0000 | APIRC_OK                 | No error.                | No action necessary.                                                                                                           |
| 1       | 0x0001 | APIRC_NO_SESSION         | Session not open.        | You must call CMUAPI_OpenSession before any CMUAPI_Command and before a CMUAPI_CloseSession command.                           |
| 2       | 0x0002 | APIRC_USER_NOT_LOGGED    | User not logged in.      | Verify the existence of an RSD file name equal to the userid and verify that it contains a password equal to that of the user. |
| 3       | 0x0003 | APIRC_SHUTDOWN_FAILED    | Shutdown command failed. |                                                                                                                                |
| 4       | 0x0004 | APIRC_SHUTDOWN_REFUSED   | Shutdown command denied. |                                                                                                                                |
| 5       | 0x0005 | APIRC_SYSTEM_DOWN        | System down.             | No action necessary.                                                                                                           |
| 6       | 0x0006 | APIRC_SYSTEM_QUIESCING   | System coming down.      | No action necessary.                                                                                                           |
| 7       | 0x0007 | APIRC_START_FAILED       | Start command failed.    |                                                                                                                                |
| 8       | 0x0008 | APIRC_STOP_FAILED        | Stop command failed.     |                                                                                                                                |
| 9       | 0x0009 | APIRC_TRACE_FAILED       | Trace command failed.    |                                                                                                                                |
| 10      | 0x000A | APIRC_UNEXPECTED_MESSAGE | Unexpected message.      |                                                                                                                                |
| 16      | 0x0010 | APIRC_GETHOST            | gethostbyname failed.    |                                                                                                                                |

| Decimal | Hex    | Error Text                  | Description                                   | Action |
|---------|--------|-----------------------------|-----------------------------------------------|--------|
| 32      | 0x0020 | APIRC_OUT_OF_MEMORY         | Out of memory.                                |        |
| 256     | 0x0100 | APIRC_SOCKET                | Socket creation failed.                       |        |
| 257     | 0x0101 | APIRC_CONNECT               | Socket connect failed.                        |        |
| 258     | 0x0102 | APIRC_SEND                  | Internal send error.                          |        |
| 259     | 0x0103 | APIRC_RECV                  | Internal receive error.                       |        |
| 260     | 0x0104 | APIRC_CHECKIN               | Internal checkin error.                       |        |
| 512     | 0x0200 | APIRC_INVALID_CMD           | Invalid API command.                          |        |
| 768     | 0x0300 | APIRC_LIST_FAIL             | List command failed.                          |        |
| 769     | 0x0301 | APIRC_ADD_FAIL              | Add command failed.                           |        |
| 770     | 0x0302 | APIRC_EXTRACT_FAIL          | Extract command failed.                       |        |
| 771     | 0x0303 | APIRC_DELETE_FAIL           | Delete command failed.                        |        |
| 772     | 0x0304 | APIRC_ERASE_FAIL            | Erase command failed.                         |        |
| 773     | 0x0305 | APIRC_STATUS_FAIL           | Status command failed.                        |        |
| 774     | 0x0306 | APIRC_SESSION_FAIL          | Session command failed.                       |        |
| 1024    | 0x0400 | APIRC_LOGIN_OK              | Login succeeded.                              |        |
| 1025    | 0x0401 | APIRC_LOGIN_FAILED          | Login failed.                                 |        |
| 1281    | 0x0501 | APIRC_GETDATA_FAILED        | GetData callback failed.                      |        |
| 1537    | 0x0601 | APIRC_ADDCARD_MISSIN<br>G   | <b>\$\$ADD</b> card missing in file.          |        |
| 1538    | 0x0602 | APIRC_ADDCARD_TO_LON<br>G   | <b>\$\$ADD</b> card to long.                  |        |
| 1539    | 0x0603 | APIRC_ADDCARD_NO_RE<br>CSEP | <b>\$\$ADD</b> card missing record separator. |        |
| 1540    | 0x0604 | APIRC_ID_REQUIRED           | Remote ID required.                           |        |
| 1541    | 0x0605 | APIRC_BID_REQUIRED          | Batch ID required.                            |        |
| 1542    | 0x0606 | APIRC_NO_ID_WILDCARD        | Wildcards in ID invalid.                      |        |
| 1543    | 0x0607 | APIRC_NO_BID_WILDCAR<br>D   | Wildcards in batch ID invalid.                |        |
| 1544    | 0x0608 | APIRC_BATCH_NO_INVALI<br>D  | Batch number invalid.                         |        |
| 1792    | 0x0700 | APIRC_SPLIT_TOO_SMALL       | Splitcount parm too small.                    |        |
| 1793    | 0x0701 | APIRC_NO_ACDLIST            | AcdList not specified.                        |        |



| Decimal | Hex    | Error Text             | Description                                       | Action |
|---------|--------|------------------------|---------------------------------------------------|--------|
| 1794    | 0x0702 | APIRC_CONNECT_FAIL     | Connect command failed.                           |        |
| 1795    | 0x0703 | APIRC_REFRESH_FAIL     | Refresh command failed.                           |        |
| 2048    | 0x0800 | APIRC_BATCH_ID_INVALID | Batch security failed batch.                      |        |
| 2049    | 0x0801 | APIRC_BATCH_ID_FAILED  | Failed batch security check.                      |        |
| 2304    | 0x0900 | APIRC_INVALID_DATETIME | Invalid date/time.                                |        |
| 2560    | 0x0A00 | APIRC_FUNC_NOTALLOWED  | Command Rejected by API Function Initiation EXIT. |        |

## Auto Connect Status Codes

The Sterling Connect:Enterprise auto connect status codes are as follows:

| Decimal | Hex    | Error Text                | Description                                                                                                 | Action |
|---------|--------|---------------------------|-------------------------------------------------------------------------------------------------------------|--------|
| 0       | 0x0000 | AC_SUCCESS                | Auto connect OK.                                                                                            |        |
| 224     | 0x00E0 | AC_BP_START_FAILED        | The Sterling B2B Integrator business process could not be started.                                          |        |
| 210     | 0x00D2 | AC_STOPPED                | Autoconnect stopped by cmustop.                                                                             |        |
| 225     | 0x00E1 | AC_ADD_FAILED_SSL         | FTP put failed due to SSL.                                                                                  |        |
| 226     | 0x00E2 | AC_REQUEST_FAILED_SSL     | FTP get failed due to SSL.                                                                                  |        |
| 227     | 0x00E3 | AC_CMD_FAILED_SSL         | FTP command failed due to SSL.                                                                              |        |
| 228     | 0x00E4 | AC_SSL_NEGOTIATION_FAILED | AUTH not supported by remote or SSLHandshake failure.                                                       |        |
| 229     | 0x00E5 | AC_SCRIPT_USER_ERROR      | Error during execution of FTPSCRIPT firewall navigation sending USER ID and password.                       |        |
| 230     | 0x00E6 | AC_SCRIPT_OPEN_ERROR      | Error establishing a session during FTPSCRIPT firewall navigation; OPEN IP address and port command failed. |        |

| Decimal | Hex    | Error Text                        | Description                                                                                                                                                  | Action                                                                                                                                                                                                                                                                       |
|---------|--------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 231     | 0x00E7 | AC_SCRIPT_SYNTAX_ERROR            | Error in one or more FTPSCRIPT firewall navigation entries, or in processing the Session Start, Pre-Send, Pre-Receive, Post-Receive, or Session End command. |                                                                                                                                                                                                                                                                              |
| 232     | 0x00E8 | AC_ERROR_INTERACTING_WITH_COMMD   | Error interacting with comm daemon.                                                                                                                          | This error can occur when the communications daemon exits without sending back a status code to Auto Connect daemon. The directory from which the system was started should be checked for presence of any core files. If the error persists, contact IBM Customer Services. |
| 233     | 0x00E9 | AC_SYSTEM_RESOURCE_ERROR          | fork, shmat, socket, etc. failed.                                                                                                                            |                                                                                                                                                                                                                                                                              |
| 234     | 0x00EA | AC_BSC_JES2_LOGON_FAILED          | JES2 signon failed.                                                                                                                                          |                                                                                                                                                                                                                                                                              |
| 235     | 0x00EB | AC_BSC_ERROR_DIALING              | Error during bisync dial.                                                                                                                                    |                                                                                                                                                                                                                                                                              |
| 236     | 0x00EC | AC_BSC_ERROR_INSTALL              | Error during bisync install.                                                                                                                                 |                                                                                                                                                                                                                                                                              |
| 237     | 0x00ED | AC_BSC_ERROR_PORTSETUP            | Error during bisync port setup.                                                                                                                              |                                                                                                                                                                                                                                                                              |
| 238     | 0x00EE | AC_ERROR_CONNECTING_WITH_COMMD    | Error connecting with comm daemon.                                                                                                                           |                                                                                                                                                                                                                                                                              |
| 239     | 0x00EF | AC_ERROR_CREATING_SOCKET          | Error creating socket.                                                                                                                                       |                                                                                                                                                                                                                                                                              |
| 240     | 0x00F0 | AC_SPECIFIED_COMMDAEMON_NOT_FOUND | Comm daemon not found.                                                                                                                                       |                                                                                                                                                                                                                                                                              |
| 241     | 0x00F1 | AC_NO_DAEMONS_FOR_PROTOCOL        | No Comm daemons for protocol.                                                                                                                                |                                                                                                                                                                                                                                                                              |
| 242     | 0x00F2 | AC_FAILED_TO_GET_SCRIPT           | Error while receiving script.                                                                                                                                |                                                                                                                                                                                                                                                                              |
| 243     | 0x00F3 | AC_RSD_ERROR                      | Syntax error in RSD file. Or, the ACD file specifies a remote that does not have a corresponding RSD file.                                                   | Run <b>cmucheckcfg</b> on the ACD and the RSD files for more specific information.                                                                                                                                                                                           |

| Decimal | Hex    | Error Text                 | Description                                                                                                                                                                                   | Action                                                                                                                                                                                                                                                                                                                                                  |
|---------|--------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 244     | 0x00F4 | AC_SETUP_FAILED            | Auto connect setup failure.                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                         |
| 245     | 0x00F5 | AC_SYNTAXERR               | Syntax error in ACD file.                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                         |
| 246     | 0x00F6 | AC_ADDFAILED_BATCHSECURITY | Add failed due to Batch Security.                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                         |
| 247     | 0x00F7 | AC_FAILED                  | Auto connect failed.                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                         |
| 248     | 0x00F8 | AC_LOGIN_FAILED            | Auto connect login failed.                                                                                                                                                                    | Verify that the password for the login account on the remote node matches the RMT_PASSWORD specified in the RSD file or the PASSWORD specified, if RMT_PASSWORD is not specified. Verify that the ADDRESS specified in the ACD file matches the name of the remote host. Run <b>cmucheckcfg</b> on the ACD and RSD files for more specific information. |
| 249     | 0x00F9 | AC_DEVICE_NOT_FOUND        | Resource not found.                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                         |
| 250     | 0x00FA | AC_PROTOCOL_ERROR          | Transmission error.                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                         |
| 251     | 0x00FB | AC_REQUEST_FAILED          | Request (extract) failed. For example, there are no requestable batches in the mailbox specified by SENDID in the ACD file (or the mailbox specified by REMOTE=, if SENDID is not specified). |                                                                                                                                                                                                                                                                                                                                                         |
| 252     | 0x00FC | AC_ADD_FAILED              | Add failed.                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                         |
| 253     | 0x00FD | AC_CONNECT_FAILED          | Connection call failed.                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                         |
| 254     | 0x00FE | AC_DEVICE_ERROR            | Port error.                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                         |
| 255     | 0x00FF | AC_DEVICE_BUSY             | Port busy.                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                         |

## Remote Connect Status Codes

The Sterling Connect:Enterprise remote connect status codes are as follows:

| Decimal | Hex    | Error Text                        | Description                                                                                   |
|---------|--------|-----------------------------------|-----------------------------------------------------------------------------------------------|
| 0       | 0x0000 | RC_SUCCESS                        | Successful remote connect.                                                                    |
| 102     | 0x0067 | RC_SSL_DISALLOWED                 | SSL disallowed, but client tried SSL login.                                                   |
| 103     | 0x0067 | RC_SSL_REQUIRED                   | SSL required, but client tried non-SSL login.                                                 |
| 104     | 0x0068 | RC_ADD_FAILED_SSL                 | FTP put failed due to SSL.                                                                    |
| 105     | 0x0069 | RC_REQUEST_FAILED_SSL             | FTP get failed due to SSL.                                                                    |
| 106     | 0x006A | RC_CMD_FAILED SSL                 | FTP command failed due to SSL.                                                                |
| 108     | 0x006C | RC_CONNECT_TO_CONTROL             | Bisync Child Daemon Connect to Control Daemon error.                                          |
| 109     | 0x006D | RC_BISYNC_SSI_ERROR               | Internal Bisync SSI error.                                                                    |
| 110     | 0x006E | RC_IO_ERROR                       | IO error.                                                                                     |
| 111     | 0x006F | RC_TIMEOUT                        | Inactivity timeout.                                                                           |
| 112     | 0x0070 | RC_BISYNC_LOST_DSR                | Bisync lost DSR error.                                                                        |
| 113     | 0x0071 | RC_DELETE_FAILED                  | Delete failed.                                                                                |
| 114     | 0x0072 | RC_LIST_FAILED                    | List failed.                                                                                  |
| 115     | 0x0073 | RC_BISYNC_TRANSMIT_ERROR          | Bisync transmit error.                                                                        |
| 116     | 0x0074 | RC_BISYNC_RECORD_TRUNCATION       | Error during Read due to truncation. Receive buffer is too small for the incoming data block. |
| 117     | 0x0075 | RC_BISYNC_RECEIVE_ERROR           | OPREAD/STDREAD failure during PARSE state.                                                    |
| 119     | 0x0077 | RC_FAILED_TO_CREATE_SEM           | Create Semaphore system call failed.                                                          |
| 120     | 0x0078 | RC_SESSINIT_EXIT_FAILED           | Session Initialization Exit failed.                                                           |
| 121     | 0x0079 | RC_INVALID_PASSWD                 | Invalid password supplied by remote.                                                          |
| 122     | 0x007A | RC_FAILED_TO_CONNECT_WITH_MAILBOX | Connect socket system call to mailbox daemon failed.                                          |
| 123     | 0x007B | RC_FAILED_TO_MODIFY_SHARED MEM    | Error returned on a Shared Memory related system call.                                        |
| 124     | 0x007C | RC_ADDFAILED_BATCHSECURITY        | Add failed due to Batch Security.                                                             |
| 125     | 0x007D | RC_REQUEST_FAILED                 | Request failed.                                                                               |
| 126     | 0x007E | RC_ADD_FAILED                     | Add failed.                                                                                   |
| 127     | 0x007F | RC_RMTCMD_FAILED                  | Failed to execute remote command.                                                             |

---

## Utilities Exit Codes

The following are the Sterling Connect:Enterprise Utilities exit codes:

| Code     | Description                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0        | Success                                                                                                                                                                                                           |
| 1        | Invalid option supplied on Command line.                                                                                                                                                                          |
| 2        | Login failed. Invalid userid or password supplied.                                                                                                                                                                |
| 3        | Hostname not specified. Host where Control daemon is running.                                                                                                                                                     |
| 4        | Port number not specified. Port on which Control daemon is listening.                                                                                                                                             |
| 5        | Invalid number of columns (option -x or --cols).                                                                                                                                                                  |
| 6        | Invalid number of rows (option -y or --rows).                                                                                                                                                                     |
| 7        | Number of files supplied on <b>cmuadd</b> is greater than 32 ( <b>cmuadd</b> only).                                                                                                                               |
| 8        | No batches match selection criteria.                                                                                                                                                                              |
| 9        | Out of disk space error ( <b>cmuadd</b> only).                                                                                                                                                                    |
| 10.11.12 | Sterling Connect:Enterprise general errors. For example, input file does not exist for cmuadd, Sterling Connect:Enterprise database error for cmuadd/cmextract/cmstatus, batch data file not found for cmextract. |
| 13       | System not up or invalid hostname or invalid port.                                                                                                                                                                |
| 14       | Could not create or open output file ( <b>cmuextract</b> only).                                                                                                                                                   |
| 15       | Could not create or open report file ( <b>cmuextract</b> only).                                                                                                                                                   |
| 16       | Could not create or open end data file ( <b>cmuextract</b> only).                                                                                                                                                 |
| 17       | Invalid date or time specified on command line.                                                                                                                                                                   |
| 18       | Internal API error sending command to the control daemon.                                                                                                                                                         |
| 19       | Invalid session ID specified.                                                                                                                                                                                     |
| 20       | Invalid flags on command line.                                                                                                                                                                                    |
| 21       | No batches were added during cmuadd.                                                                                                                                                                              |

---

## Authorization Log Message IDs

The general format of entries in the auth.log file is:

```
Timestamp hostnamemessage-ID qualifying-text : message-short-text
```

The qualifying text string contains specific information about the event, such as the account or policy name affected. Some entries do not have qualifying text information.

| Message ID | Qualifying Text                        | Message Short Text                                                                                                                                                                                                                                                                                                                                                                |
|------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0001   | Login OK                               | A user login was processed successfully. The user name is indicated as rsd="user name." If policy controls were applied, then the policy name is indicated as policy="policy name."                                                                                                                                                                                               |
| AUTH0002   | Login OK with warning                  | A user login was processed successfully, but a warning was issued because of settings in the users' policy file. The user name is indicated as rsd="user name." The warning is logged in an AUTH0009 entry that precedes this entry in the log.                                                                                                                                   |
| AUTH0003   | Login FAILED, ID and/or pwd incorrect  | A user login failed verification of the user ID and password. The user ID or the password, or both, may be invalid. The user name is indicated as rsd="user name."                                                                                                                                                                                                                |
| AUTH0004   | Login FAILED, account is locked        | A user login failed because the account associated with the user ID is locked. The account may have been locked by the administrator (see AUTH0060), or it may have become locked because of too many consecutive login attempts using an incorrect password (see AUTH0062). The user name is indicated as rsd="user name." The policy name is indicated as policy="policy name." |
| AUTH0005   | Login FAILED, password is expired      | A user login failed because the account password is expired. The user can login after successfully changing their password, if the account policy controls allow this. The user name is indicated as rsd="user name." The policy name is indicated as policy="policy name."                                                                                                       |
| AUTH0006   | Login FAILED, password change required | A user login failed because the administrator has set "password change required" for the account. The user can login after successfully changing their password if the account policy controls allow this. The user name is indicated as rsd="user name." The policy name is indicated as policy="policy name."                                                                   |

| Message ID | Qualifying Text                           | Message Short Text                                                                                                                                                                                                                                                    |
|------------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0007   | Login FAILED, cannot read rsdpolicy file  | A user login has failed due to an error reading the account policy file. This error results if the account policy file is corrupt, or if the system POLICY_LEVEL = 2 (see AUTH0072) and no account policy file exists. The user name is indicated as rsd="user name." |
| AUTH0008   | Login FAILED, cannot write rsdpolicy file | A user login has failed due to an error writing the account policy file. This is an internal error. The user name is indicated as rsd="user name." The policy name is indicated as policy="policy name."                                                              |
| AUTH0009   | Warning issued by account policy          | A warning was issued for a user login because of the parameters in the accounts' policy file. The user name is indicated as rsd="user name." The warning text appears in this log entry.                                                                              |

## Policy File Entries

| Message ID | Qualifying Text            | Message Short Text                                                                                                                                                                                                                                                 |
|------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0020   | Policy created             | The administrator created a policy file. The policy name is indicated as policy="policy name."                                                                                                                                                                     |
| AUTH0021   | Policy creation failed     | An error occurred creating a policy file. The policy name is indicated as policy="policy name." The failure could be due to invalid parameters in the creation request (such as MIN password length > Max password length).                                        |
| AUTH0022   | Policy Modified            | The administrator modified an existing policy file. The policy name is indicated as policy="policy name."                                                                                                                                                          |
| AUTH0023   | Policy Modification Failed | An error occurred modifying a policy file. The policy name is indicated as policy="policy name." The failure could be due to invalid parameters in the modify request (for example, MIN password length > Max password length), or the policy name may be invalid. |
| AUTH0024   | Policy deleted             | The administrator deleted a policy file. The policy name is indicated as policy="policy name."                                                                                                                                                                     |
| AUTH0025   | Policy deletion failed     | An error occurred deleting a policy file. The policy name is indicated as policy="policy name." The failure could be due to an invalid policy name in the request.                                                                                                 |

## Rsdpolicy File Entries

| Message ID | Qualifying Text                | Message Short Text                                                                                                                                                                                                                    |
|------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0040   | Rsdpolicy created              | The administrator created an rsdpolicy file. The account name is indicated as rsd="user name."                                                                                                                                        |
| AUTH0041   | Rsdpolicy creation failed      | An error occurred creating an rsdpolicy file. The failure could be due to an invalid account name, or an invalid policy name. The policy name is indicated as policy="policy name." The account name is indicated as rsd="user name." |
| AUTH0042   | Rsdpolicy modified             | The administrator modified an rsdpolicy file. The account name is indicated as rsd="user name."                                                                                                                                       |
| AUTH0043   | Rsdpolicy modification failed. | An error occurred modifying an rsdpolicy file. The failure could be due to an invalid account name, or a missing or corrupted rsdpolicy file. The account name is indicated as rsd="user name."                                       |
| AUTH0044   | Rsdpolicy file deleted         | The administrator deleted an rsdpolicy file. The account name is indicated as rsd="user name."                                                                                                                                        |
| AUTH0045   | Rsdpolicy deletion failed      | An error occurred deleting an rsdpolicy file. The failure could be due to an invalid account name. The account name is indicated as rsd="user name."                                                                                  |

## Account Lock-Related Entries

| Message ID | Qualifying Text                              | Message Short Text                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0060   | Account LOCKED by administrator              | The administrator has locked an account. The account name is indicated as rsd="user name." Locking the account prevents the user from logging in or changing their password.                                                                                                                                                                                                                                                                               |
| AUTH0061   | Account UNLOCKED by administrator            | The administrator has unlocked an account. The account name is indicated as rsd="user name."                                                                                                                                                                                                                                                                                                                                                               |
| AUTH0062   | Account locked by consecutive login failures | An account was locked because the maximum number of consecutive login failures specified in the rsdpolicy file was exceeded. The account name is indicated as rsd="user name." The policy name is indicated as policy="policy name." Only login attempts that fail due to an incorrect password are counted as failures. A successful login resets the login failure count. Locking the account prevents the user from logging in or changing her password |



## Policy Level Entries

| Message ID | Qualifying Text                       | Message Short Text                                                                                                                                                                                                                                                                                                                                            |
|------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0070   | POLICY_LEVEL=0 (Disallowed) in effect | The current password administration policy level is 0. This policy level causes account policy controls to be ignored during login and password change processing. This message is logged when the system is initialized, and when the policy level is changed.                                                                                               |
| AUTH0071   | POLICY_LEVEL=1 (Optional) in effect   | The current password administration policy level is 1. This policy level causes account policy controls to be enforced only for accounts where an rsdpolicy files exists. Accounts not having an rsdpolicy file are treated as if POLICY_LEVEL=0 were in effect. This message is logged when the system is initialized, and when the policy level is changed. |
| AUTH0072   | POLICY_LEVEL=2 (Required) in effect   | The current password administration policy level is 2. This policy level causes account policy controls to be enforced for all accounts. Accounts not having an rsdpolicy file are prevented from logging in. This message is logged when the system is initialized, and also when the policy level is changed.                                               |

## Password Change Entries

| Message ID | Qualifying Text                           | Message Short Text                                                                                                                                                                                                                                                                                   |
|------------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0080   | Password Changed                          | An account password has been changed. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                                                |
| AUTH0081   | Password change FAILED, new pwd too long  | A password change attempt has failed because the new password specified exceeds the maximum password length specified in the account policy. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.         |
| AUTH0082   | Password change FAILED, new pwd too short | A password change attempt has failed because the new password specified is shorter than the minimum password length specified in the account policy. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator. |

| <b>Message ID</b> | <b>Qualifying Text</b>                              | <b>Message Short Text</b>                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0083          | Password change FAILED, account is locked           | A password change attempt by a user has failed because the account is locked. The account name is indicated as rsd="user name." Locking an account prevents the user changing her own password, but the administrator is allowed to change the password.                                                                                                                            |
| AUTH0085          | Password change FAILED, password hard expired       | A password change attempt by a user has failed because the account password is expired, and the account policy specifies DURATION=0. The password change by user is disallowed in this case because the account would still be expired after the change. The administrator is allowed to change the users' password in this case. The account name is indicated as rsd="user name." |
| AUTH0086          | Password change FAILED, file system error           | A password change attempt has failed due to file system error. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                                                                                                      |
| AUTH0087          | Password change FAILED, new pwd in history          | A password change attempt by a user has failed because the new password is in the accounts' password history. The password history check is bypassed when the users' password is changed by the administrator. The account name is indicated as rsd="user name."                                                                                                                    |
| AUTH0088          | Password change FAILED, ID and/or old pwd incorrect | A password change attempt by a user has failed because the old password specified was not correct, or the account name supplied is incorrect. The account name is indicated as rsd="user name."                                                                                                                                                                                     |
| AUTH0089          | Password change FAILED, error reading rsdpolicy     | A password change attempt has failed due to an error reading the account policy file. The error could be caused by a corrupted account policy file. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                 |
| AUTH0090          | Password change FAILED, error writing rsdpolicy     | A password change attempt has failed due to an error writing the account policy file. The error could be caused by a file system problem. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                           |

| Message ID | Qualifying Text                                                                       | Message Short Text                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0091   | Password change FAILED, internal error occurred                                       | A password change attempt has failed due to an internal error. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                                                                                                                                           |
| AUTH0092   | Password change FAILED, new pwd same as old                                           | A password change attempt has failed because the old and new passwords supplied in the request are the same. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                                                                                             |
| AUTH0093   | Password change FAILED, error extracting old pwd from rsd                             | A password change attempt has failed because the old passwords could not be extracted from the rsd file. This is most likely caused by an incorrect account name in the request. The account name is indicated as rsd="user name." The message text indicates whether the change was initiated by the user or the administrator.                                                                                         |
| AUTH0094   | Password change FAILED, could not parse RSD file                                      | A password change attempt has failed because the rsd file for the account could not be parsed. This is most likely caused by an incorrect account name in the request, but could also be caused by a syntax error in the rsd file. The account name is indicated as rsd="user name". The message text indicates whether the change was initiated by the user or the administrator.                                       |
| AUTH0095   | Password change FAILED, External Authentication server unavailable                    | A password change attempt has failed because the External Authentication server is unavailable. The account is configured to authenticate via the External Authentication server. The most likely cause is that the External Authentication server has not been started. The account name is indicated as rsd="user name". The message text indicates whether the change was initiated by the user or the administrator. |
| AUTH0096   | Password change FAILED, ADMIN change not allowed with External Authentication account | A password change attempt has failed because an administrator attempted to change the password for an account configured to authenticate via the External Authentication server. Administrator password change is not allowed for such accounts. The account name is indicated as rsd="user name".                                                                                                                       |
| AUTH0097   | Password change FAILED, error sending request to External Authentication server       | A password change attempt has failed because an error was encountered in sending the request to the External Authentication server. The account is configured to authenticate via the External Authentication server. The account name is indicated as rsd="user name".                                                                                                                                                  |

| <b>Message ID</b> | <b>Qualifying Text</b>                                                | <b>Message Short Text</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0098          | Password change FAILED by External Authentication server              | A password change attempt has been failed by the External Authentication server. The account is configured to authenticate via the External Authentication server. The most likely cause is that the old password supplied for the account was incorrect. The account name is indicated as rsd="user name".                                                                                                                                                                                                                                                                 |
| AUTH0099          | Password changed by External Authentication server                    | An account password has been changed by the External Authentication server. The account is configured to authenticate via the External Authentication server. This message normally appears as a group of consecutive messages in the log. The first message of the group indicates the account name as rsd="user name", and includes the text above. It is followed by one or more additional messages having the same message ID and timestamp, and including information about the Distinguished Name involved in the request and the authentication server(s) accessed. |
| AUTH0100          | Login FAILED, External Authentication server is unavailable           | A login attempt has failed because the External Authentication server is unavailable. The account is configured to authenticate via the External Authentication server. The most likely cause is that the External Authentication server has not been started. The account name is indicated as rsd="user name".                                                                                                                                                                                                                                                            |
| AUTH0101          | Login FAILED, error sending request to External Authentication server | A login attempt has failed because an error was encountered in sending the request to the External Authentication server. The account is configured to authenticate via the External Authentication server. The account name is indicated as rsd="user name".                                                                                                                                                                                                                                                                                                               |
| AUTH0102          | Login FAILED, error invoking security exit                            | A login attempt has failed because an error was encountered in invoking the security exit. The account name is indicated as rsd="user name".                                                                                                                                                                                                                                                                                                                                                                                                                                |
| AUTH0103          | Login FAILED, error response from security exit                       | A login attempt has been failed by the site security exit. The configured security exit was invoked for the login, and returned a non-zero return code. The account name is indicated as rsd="user name".                                                                                                                                                                                                                                                                                                                                                                   |
| AUTH0104          | Login FAILED by External Authentication server                        | A login attempt has been failed by the External Authentication server. The account is configured to authenticate via the External Authentication server. The account name is indicated as rsd="user name".                                                                                                                                                                                                                                                                                                                                                                  |

| Message ID | Qualifying Text                                                        | Message Short Text                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0105   | Login OK by External Authentication server                             | A login has been allowed by the External Authentication server. The account is configured to authenticate via the External Authentication server. The account name is indicated as rsd="user name".                                                                                                                                                                                                                          |
| AUTH0106   | External Authentication server started                                 | The External Authentication server has been successfully started. The authentication daemon attempts to start the server when EXTERNALAUTHPATH is specified in the \$CMUHOME/mcd/control.mcd file.                                                                                                                                                                                                                           |
| AUTH0107   | The External Authentication server has terminated unexpectedly         | The External Authentication server, which was previously started by the authentication daemon, has terminated prematurely. Pending and subsequent authentication and password change requests for accounts configured to authenticate via the External Authentication server will fail. The most likely cause is that someone has killed or shutdown the server.                                                             |
| AUTH0108   | The External Authentication server has been shut down normally         | The External Authentication server, which was previously started by the authentication daemon, has been shut down normally during the course of Sterling Connect:Enterprise shutdown processing.                                                                                                                                                                                                                             |
| AUTH0109   | Connection established with External Authentication server             | The authentication daemon has successfully established a connection with the External Authentication server. The authentication daemon attempts to establish a connection to the server when EXTERNALAUTH is specified as YES or RSD in the \$CMUHOME/mcd/control.mcd file.                                                                                                                                                  |
| AUTH0110   | Secure connection established with External Authentication server      | The authentication daemon has successfully established a secure connection with the External Authentication server. The authentication daemon attempts to establish a connection to the server when EXTERNALAUTH is specified as YES or RSD in the \$CMUHOME/mcd/control.mcd file. A secure connection is indicated when the EXTERNALAUTHSPD parameter in the same file specifies an spd file with SECURITY_POLICY=REQUIRED. |
| AUTH0111   | Connection with External Authentication server terminated unexpectedly | The connection between the authentication daemon and the External Authentication server has terminated prematurely. The most likely cause is that the server has terminated. Pending and subsequent authentication and password change requests for accounts configured to authenticate via the External Authentication server will fail.                                                                                    |

| Message ID | Qualifying Text                                           | Message Short Text                                                                                                                                                                                                                                                                                                                                                                                |
|------------|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUTH0112   | connect=Y N, start=Y N,<br>Authentication server settings | This message shows the configured settings for the External Authentication server.<br><br>Connect=YES NO indicates whether the authentication daemon is to establish a connection to the server.<br><br>Start=YES NO indicates whether the authentication daemon is to start the server.                                                                                                          |
| AUTH0113   | External Authentication server startup failed             | An attempt to start the External Authentication server has failed. The most likely cause is an incorrect setting for the EXTERNALAUTHPATH or EXTERNALAUTHCONTROLPORT parameter in the \$CMUHOME/mcd.control.mcd file. You may get additional return codes as part of this messages, such as:<br>0x02 IDMBRC_INTERNAL_ERROR. Refer to <i>Additional Return Codes for AUTH0113</i> on page 262.     |
| AUTH0114   | External Authentication server connection attempt failed  | An attempt to establish a connection with the External Authentication server has failed. The most likely cause is an incorrect setting for the EXTERNALAUTHPORT or EXTERNALAUTHSECUREPORT parameter in the \$CMUHOME/mcd/control.mcd file. It is also possible that the External Authentication server has not been started if Sterling Connect:Enterprise is not configured to start the server. |

### Additional Return Codes for AUTH0113

The following messages may accompany the AUTH0113 message ID.

| Message ID | Qualifying Text        | Description                                                                                                                                                                                                        |
|------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x02       | IDMBRC_INTERNAL_ERROR  | Internal error, see additional diagnostics in trace file.                                                                                                                                                          |
| 0x03       | IDMBRC_CREATE_FAILURE  | Socket creation failure, see additional diagnostics in trace file.                                                                                                                                                 |
| 0x04       | IDMBRC_CONNECT_FAILURE | Unable to connect, retries exhausted.                                                                                                                                                                              |
| 0x05       | IDMBRC_HOST_NOT_FOUND  | The specified host is unknown, or the name is valid but does not have an IP address, a non-recoverable name server error occurred, or a temporary error occurred on an authoritative name server. Try again later. |
| 0x06       | IDMBRC_SERIALIZE_ERROR | Failure to process xml request message.                                                                                                                                                                            |

| <b>Message ID</b> | <b>Qualifying Text</b>   | <b>Description</b>                                                                         |
|-------------------|--------------------------|--------------------------------------------------------------------------------------------|
| 0x0a              | IDMBRC_WRITE_ERROR       | General socket problem, see additional diagnostics in trace file.                          |
| 0x0b              | IDMBRC_MEMORY_FAILURE    | Out of memory.                                                                             |
| 0x0d              | IDMBRC_START_FAILURE     | Could not start external authentication process, see additional diagnostics in trace file. |
| 0x0f              | IDMBRC_RESOURCE_FAILURE  | Out of memory.                                                                             |
| 0x11              | IDMBRC_XML_PARSE_FAILURE | Failure to process xml response message.                                                   |





---

# Translation Table Format

The basic character set for ASCII has only 127 characters; higher values are normally translated to periods. Some characters in EBCDIC have no representatives in ASCII and are similarly translated to periods.

If you want to translate these unrepresented characters to meaningful characters, you must create a translate table which tells the program how to handle these ASCII-to-EBCDIC or EBCDIC-to-ASCII translations.

An example of a conversion table is shown below. The table consists of 32 lines of 32 characters each. Each line represents 16 printable hexadecimal characters followed by a line feed. The first 16 lines provide information for ASCII-to-EBCDIC conversion and the second 16 lines provide the EBCDIC-to-ASCII conversion information. The table must include 32 lines.

The numeric equivalent of each incoming character is used as the zero origin index into the conversion table. This index specifies the table location containing the hexadecimal value of the converted character. For example, if the 48th position in the table contains a value of x'F0', Sterling Connect:Enterprise converts all characters with a value of 48 (x'30') to a value of 240 (x'F0').

The bold hex values in the table below indicate the changes in Sterling Connect:Enterprise to accommodate the new European monetary standard, the EURO.

|                                         |
|-----------------------------------------|
| 0001020337402E2F1605250B0C0D0E0F        |
| 101112133C3D4B4B18193F271C1D1E1F        |
| 405A7F7B5B6C507D4D5D5C4E6B604B61        |
| F0F1F2F3F4F5F6F7F8F97A5E4C7E6E6F        |
| 7CC1C2C3C4C5C6C7C8C9D1D2D3D4D5D6        |
| D7D8D9E2E3E4E5E6E7E8E9ADE0BD5F6D        |
| 79818283848586878889919293949596        |
| 979899A2A3A4A5A6A7A8A9C06AD0A107        |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B <b>9F</b> 4B4B4B4B4B4B4B4B4B4B |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B          |
| 000102032E092E7F2E2E0A0B0C0D0E0F        |
| 101112131415161718191A1B1C1D1E1F        |
| 2E2E2E2E2E0A2E1B2E2E2E2E050607          |
| 2E2E2E2E2E2E2E2E2E2E2E14152E1A          |
| 202E2E2E2E2E2E2E2E2E2E3C282B2E          |
| 262E2E2E2E2E2E2E2E2E21242A293B5E        |
| 2D2F2E2E2E2E2E2E2E7C2C255F3E3F          |
| 2E2E2E2E2E2E2E2E603A2340273D22          |
| 2E6162636465666768692E2E2E2E2E          |
| 2E6A6B6C6D6E6F7071722E2E2E2E <b>A4</b>  |
| 2E7E737475767778797A2E2E2E5B2E2E        |
| 2E2E2E2E2E2E2E2E2E2E2E2E5D2E2E          |
| 7B4142434445464748492E2E2E2E2E2E        |
| 7D4A4B4C4D4E4F5051522E2E2E2E2E2E        |
| 5C2E535455565758595A2E2E2E2E2E2E        |
| 303132333435363738392E2E2E2E2E2E        |

## Symbols

### **\$\$ADD**

A command from a remote site signaling Sterling Connect:Enterprise that a data collection function is beginning. The data that accompanies the \$\$ADD command is placed in the mailbox for later extraction or transfer.

### **\$\$DELETE**

A command from a remote site signaling Sterling Connect:Enterprise to delete a batch from the mailbox.

### **\$\$DIRECTORY**

A command from a remote site requesting Sterling Connect:Enterprise for a partial or complete list of the mailbox contents.

### **\$\$REQUEST**

A command from a remote site requesting Sterling Connect:Enterprise to send specified batches from the mailbox to its remote location.

## A

### **account**

Term used in the Sterling Connect:Enterprise for UNIX Site Administration user interface to identify a file that defines a local user's password that allows access to local user commands on Sterling Connect:Enterprise for UNIX, or a file that defines the communications and data characteristics of remote sites that are authorized to access Sterling Connect:Enterprise for UNIX. The file that contains the information for each type of account is called a Remote Site Definitions (RDS) file. See also *Remote Site Definitions File*.

## **Admin Daemon (cmuadmin)**

Daemon that communicates requests from the Sterling Connect:Enterprise Site Administration User Interface to the Service Interface Daemon (cmusvid). This enables Sterling Connect:Enterprise for UNIX to use a Java-based HTTP server, rather than requiring a third-party Web server. This daemon also manages all sessions with remote sites that use the WebDAV protocol.

## **AIX**

The IBM implementation of the UNIX operating system. The AIX operating system runs on the IBM RS/6000 line of computers.

## **API calls**

Standard C function calls that can be embedded in an application program. The IBM API subroutines are responsible for performing inter-process communication with the appropriate Sterling Connect:Enterprise components and reporting errors or normal completions back to the calling application.

## **argument**

Additional information that is passed to a command or function. For example, in the command line, `$$ADD -btext`, the command is `$$ADD` and the argument is `-btext`.

## **AS2**

Applicability Standard 2 is a transport protocol that uses HTTP to transport data over the Internet. It offers a flexible set of security measures for organizing the transfer of data between companies, including a secure HTTP connection (HTTP/S), S/MIME for data privacy, data integrity, data authenticity, and nonrepudiation.

## **AS2 Contract**

The set of data exchange parameters that are agreed on by both trading partners involved in an AS2 transfer.

## **as2report**

An operator command that reports the activity of the AS2 protocol.

## **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 ranging 0–127 decimal. An ASCII file created on a UNIX computer is readable on other kinds of computers.

## Async Daemon (cmuasyd)

One of the Communications daemons that manages all sessions established with remote sites through the Async protocols XMODEM, YMODEM, ZMODEM and Kermit.

## Async Interactive Mode

A mode of operation for the Asynchronous Communications daemon in which the remote site communicates with the Sterling Connect:Enterprise site using interactive commands. The user must provide a valid password defined in the RSD in order to log on. The nature of the session is conversational. See also *interactive*. Compare with *SPC Emulation mode*.

## asynchronous (Async)

A way of receiving or sending data that does not rely on timing to travel. Compare with *binary synchronous*. See also *protocol*.

## Authentication Server Daemon (cmuauthd)

The authentication server daemon enforces password policies when a user logs on to Sterling Connect:Enterprise for UNIX. It first checks the password administration configuration file and determines how whether a password policy is enforced, then it determines how to enforce the policy using information in the password administration configuration file, the password policy files, and the RSD policy files.

## auto connect

A Sterling Connect:Enterprise feature that enables host-initiated data communications to one or more remote sites. The local and remote sites may be connected using manual dial, auto dial, or non-switched, for example, leased lines. The auto connect session may be fully automated by time and day by definitions entered in the ACD, or controlled with either the \$\$CONNECT or **cmuconnect** commands. Full reporting of auto connect activity is available. See also *schedule*.

## Auto Connect Daemon (cmuacd)

The Sterling Connect:Enterprise process that parses the Auto Connect Definitions (ACD) files and initiates auto connect sessions based on scheduling information supplied therein.

## Auto Connect Definitions File (ACD)

The files containing parameters that define lists of remote sites to be contacted either manually, upon issuance of the **cmuconnect** command by a local site user or automatically by the Auto Connect Daemon in response to scheduling information they contain. There is one ACD for each auto connect. These files can be created and modified from the Sterling Connect:Enterprise for UNIX Site Administration user interface provided with Sterling Connect:Enterprise.

## **autodial**

Refers to the host computer's capability to automatically dial the remote site to establish a connection on a switched line. The autodial feature is usually generated for the local site by the ACD file. Compare with *manual dial*.

## **awk**

A UNIX programming language geared toward text manipulation.

# **B**

## **batch**

In Sterling Connect:Enterprise, a set of related data collected by or added to the mailbox - usually a file or group of files sent at one time. In UNIX, a command that lets you input many commands to run unattended in sequence.

## **BATCHID**

A parameter can be completed 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 99,999,999 assigned internally by Sterling Connect:Enterprise to each individual batch. This number can be specified in command using the BATCHID= parameter. The number may be obtained by either the \$\$DIRECTORY or the **cmulist** commands. See also *BATCHID* and *user batch ID*.

## **batch processing**

The sending of a large body of data without intervening responses from the receiving unit. Contrast with *interactive*.

## **batch security**

An optional method of providing security in Sterling Connect:Enterprise for remote site access to the system. Mailbox IDs are assigned to remote sites and defined as valid at the local site. If Batch Security is used, remote sites must supply a valid ID as part of the remote command in order to access the mailbox data files.

## **batch status**

A set of flags maintained for each batch on the mailbox. The batch status flags are displayed when you use the **cmulist** local command or the \$\$DIRECTORY or **dir** remote command. Batch status can be altered by using the **cmustatus** local command.

**baud rate**

The transmission rate of a modem, in bits per second.

**BID**

An abbreviation for the parameter BATCHID=. See *BATCHID*.

**/bin**

In UNIX, the name usually given to the directory that contains important binary and executable files. Several such */bin* subdirectories can exist within a system, each one storing the binary and executable files relevant to the program(s) stored in that directory.

In Sterling Connect:Enterprise, */bin* is a subdirectory of the *\$CMUHOME/aix*, *\$CMUHOME/sun*, and *\$CMUHOME/hpux* directories.

**binary data**

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

**binary file**

A file comprised of binary numbers (zeros and ones). A computer-readable file format that usually cannot be read directly by other computers. This type of file is often a computer program file, such as an executable or command driver, that has been translated by a compiler into a language, sometimes called machine language, that a computer can read.

**binary synchronous (Bisync)**

A standard protocol used to transmit blocks of data over telecommunications lines between local and remote sites. This is one of the line protocols used by Sterling Connect:Enterprise.

**blank compression**

A method of replacing strings of contiguous blanks with control characters indicating the number of blanks removed. Commonly used to shorten the amount of data sent over telecommunications lines. Sterling Connect:Enterprise uses standard 3780 blank compression techniques on Bisync lines.

**blank truncation**

A method of dropping trailing blanks from the end of fixed length data records before sending the data over telecommunications lines. Used by Sterling Connect:Enterprise for Bisync connections as an option to shorten the amount of data sent over telecommunications lines.

## **block**

The fundamental unit of information used for access and storage allocation on a mass storage medium. The size of the block varies between implementations and file systems. On media such as 9-track tape that write variable length strings of data, block is the size of those strings. Block is distinguished from record; a block contains several records, whereas the number of records denotes the blocking factor.

## **blocking**

The process of combining more than one logical record of data within a single packet or string of transmitted bytes. Blocked data records are usually separated by a unique record separator character that does not occur within the data records themselves.

## **block size**

The total length of a packet or block of data, containing one or more logical records, including the protocol-specific header and trailer strings that envelope the data being transmitted.

## **Bisync**

See *binary synchronous*.

## **Bisync Daemon (cmubscd)**

One of the Communications daemons that manages all sessions established with remote sites through the Bisync (binary synchronous, or Bisync) 3780/2780 protocols.

## **BSCRTDIR**

A Sterling Connect:Enterprise environment variable that defines the directory where the Bisync Runtime library is installed.

## **buffer**

A storage space in computer memory where data is stored temporarily into convenient units for system operations. Buffers are often used by programs, such as editors, that access and alter text or data frequently.

## **business process**

A business process is the method used by Sterling B2B Integrator to determine the order of events that occur when integrating data between applications. Business processes are based on a specialized form of Extensible Markup Language (XML) called Business Process Markup Language (BPML).

## **byte**

A fundamental unit of data made up of bits. In most cases, a byte is made up of eight bits.



## C

### **call**

See *system call* and *API calls*.

### **ceinstall**

A shell script used to install Sterling Connect:Enterprise from the distribution media.

### **ceuacq**

An operator command that displays the current entries in the auto connect queue and allows users to query the status and change the priority of individual entries.

### **ceupassadm**

Command that enables administrators to create and maintain password policy files and RSD policy files.

### **ceupassrpt**

Command that enables administrators to display RSD policy files according to expiration date or by the password policy that generated the RSD policy file.

### **ceupasswd**

A local user command that enables users to change their password.

### **ceuqdel**

An operator command that deletes the auto connect queue database.

### **ceushutdown**

A local-site command asking Sterling Connect:Enterprise to begin the system shutdown procedure and end its processing.

### **ceustartup**

A UNIX shell script to start the Sterling Connect:Enterprise system. It starts up all of the core daemons (Mailbox, Control, Exits, Log, Auto Connect) and the installed communications daemons.

### **ceutrace**

An administrator command that turns tracing on and off and set tracing levels without restarting Sterling Connect:Enterprise. You can also use **ceutrace** to view the current settings. Refer to the following procedures in this section:

### **child process**

Also called children. A new process started by a parent process through a fork. Resources of the parent process are shared by the children. Every UNIX process is a child of another process, except for *init*. See also *fork*, *orphan*, and *parent process*.

### **client-server**

An architecture wherein a task is divided into two separate entities, a client and a server. The client and server can run on different computers on the LAN, and communicate with each other to perform tasks. The client always requests services from the server. The Sterling Connect:Enterprise architecture is based on this paradigm.

### **cmuadd**

A local-site command asking Sterling Connect:Enterprise to add specified batches to the mailbox.

### **cmuconnect**

A local-site command asking Sterling Connect:Enterprise to activate the Sterling Connect:Enterprise auto connect feature for a previously defined list of remote sites (specified in an Auto-Connect definitions file). Data can be sent to and received from the remote sites during an auto connect session.

### **cmucust**

A shell script used to configure Sterling Connect:Enterprise. This shell script is called by the **ceinstall** script.

### **cmudelete**

A local-site command asking Sterling Connect:Enterprise to logically delete specified batches from the mailbox. Affected batches can be recovered by Sterling Connect:Enterprise with the **cmustatus** command after this operation.

### **cmuediintd**

The EDIINT daemon used to package and unpack AS2 messages.

### **cmuerase**

A local-site command to Sterling Connect:Enterprise to physically erase specified batches from the mailbox. Erased batches cannot be recovered.

**cmuextract**

A local-site command to Sterling Connect:Enterprise to retrieve a copy of the specified batches from the mailbox, decompress them (where necessary), and place them in a designated area.

**CMUHOME**

A Sterling Connect:Enterprise environment variable that defines the home or destination directory of all the Sterling Connect:Enterprise files.

**CMUHOST**

A Sterling Connect:Enterprise environment variable that defines the host name where the Sterling Connect:Enterprise control daemon (*cmuctld*) is running.

**cmuhttpd**

A specialized HTTP daemon used for sending and receiving packaged AS2 messages.

**cmulist**

A local-site command asking Sterling Connect:Enterprise to list specified batches in the mailbox.

**CMUPASWD**

A Sterling Connect:Enterprise environment variable that defines user IDs for the mailbox. If CMUPASWD is not specified, you will be prompted for a password each time you invoke a Sterling Connect:Enterprise utility.

**CMUPORT**

A Sterling Connect:Enterprise environment variable that defines the TCP/IP port number of the control daemon (*cmuctld*).

**cmurefresh**

A local-site command that instructs Sterling Connect:Enterprise to re-examine all auto connect lists and update that information. This command is issued each time the administrator adds a new or modifies an existing ACD file. This command is also used to refresh the AS2 configuration file.

**cmusession**

A local-site command that produces a formatted report on the status of all communications and Auto Connect daemon activity.

**cmustatus**

A local-site command allowing the Sterling Connect:Enterprise system administrator to change batch status flags through the system console.

### **cmustop**

A local-site command used to stop a communications daemon, a child process spawned by a communications daemon, or an auto connect session.

### **cmutrace**

A local-site command enabling the Sterling Connect:Enterprise system administrator to start or stop a trace on specified RTIC daemon sessions. This command does not apply to the Cleo bisync daemon.

### **command**

An instruction sent to the computer shell. A typical command consists of the utility name followed by the arguments that are passed to the utility. For example, in the command line, \$\$ADD -btext, the command is \$\$ADD and the argument is -btext.

### **command line**

One or more commands, arguments, and options strung together to create a command.

### **Communication Ports Definition File (CPD)**

The files that define for each communications daemon (Async, Bisync, or FTP) the resources (ports or devices) available to that daemon and for which that daemon is responsible.

### **Communications Daemon(s)**

The Sterling Connect:Enterprise process that coordinates all communications between local and remote sites. Three types of daemons are available, each one handling a separate communications protocol: Bisync, Async, and FTP. More than one of these daemons can be present simultaneously.

### **compressed file**

A file that has been shrunk by compression software to less than its original size. See also *blank compression*.

### **compression**

A technique by which data in a particular format is made to occupy less space on a storage device or within transmitted strings by reducing re-occurring instances of like-valued bytes to shortened representations of same. These shorter representations must later be interpreted by a decompression method that expands the data back to its original size without imposing loss of the original content. See also *blank compression*.

**console**

The main terminal, displaying all the system error messages and serving as the central control panel for the system. More generally, the terminal used by the system administrator.

**Control Daemon (cmuctld)**

The Sterling Connect:Enterprise process that orchestrates TCP/IP communications between all the product's daemons. It also parses the Mailbox Control Definitions (MCD) file at startup and the Remote Site Definitions (RSD) files when auto connects or remote connects are initiated.

**cpio**

A UNIX command that creates file archives and allows extraction of individual files from those archives. Sterling Connect:Enterprise is distributed as a cpio file.

**cron**

A UNIX command used to schedule routine and regular tasks such as file backup. In Sterling Connect:Enterprise, one of the commands embedded in the Remote Site Definition file that enables time/date scheduling for transmission and reception of data.

**/crontab**

The file that contains the settings for the **cron** command.

## D

**daemon**

A process that performs a particular task in the background without user intervention. In Sterling Connect:Enterprise, one of several parts of the program responsible for a particular task (for example, the Mailbox daemon, the Control daemon, the Communications daemons, the Exits daemon, the Log daemon, and the Auto Connect daemon).

**data bits**

The number of bits used by Async communications protocols to transmit a single character.

**data collection**

The process in which Sterling Connect:Enterprise collects data from remote sites and stores it in the mailbox. Data collection means data is input from a remote site to Sterling Connect:Enterprise at the host computer.

### **data transmission**

The process in which Sterling Connect:Enterprise transmits data from the Mailbox batch files to remote sites. Data transmission means data is output from Sterling Connect:Enterprise at the host computer to the remote site.

### **debug**

The process of locating and correcting errors in computer programs.

### **default**

A value or state assumed when no other value or state is supplied.

### **definition file**

A file that defines conditions for a function, operation, or component. In Sterling Connect:Enterprise, the definition files are Mailbox Engine (MED), Mailbox Control (MCD), Remote Site (RSD), Communication Ports (CPD), and Auto Connect (ACD). These files can be created and modified from the Site Administration user interface provided with Sterling Connect:Enterprise.

### **del**

The FTP command that, in Sterling Connect:Enterprise, enables a remote site to delete specified batches from the mailbox.

### **dependent**

Term used in role-based access to identify the relationship between a role and its parent role. Administrator is the parent of all roles. All roles are a dependent to Administrator. See also *role*, *parent role*.

### **destination**

The target for a directed command.

### **device**

See *physical device*.

### **dial line**

A telecommunications line on which connections are established over dial-up telephone line. Also referred to as switched line. Compare with *leased line*.

**dir**

The FTP command that, in Sterling Connect:Enterprise, enables a remote site to request the contents of the mailbox.

**directory**

A place to keep particular files on a computer; usually, computer files are stored using a series of hierarchically arranged directories. In Sterling Connect:Enterprise, a formatted listing of control information for batches on Sterling Connect:Enterprise batch files. It is obtained by using the remote site **\$\$DIRECTORY** or **dir** (in FTP), or the local site **cmulist** command.

**distributed system**

The ability of a computer program to divide tasks among several linked computers and in so doing, to expedite the program functions. In the context of Sterling Connect:Enterprise, the ability of the program to assign its daemons to several computers and still work together. See also *daemon*.

**driver**

A module that translates program instructions into instructions for specific peripheral devices. For example, a device driver allows your computer to communicate with your printer.

**dynamic linking**

The ability to resolve symbolic references at run time. Systems that use dynamic linking can execute processes without resolving unused references.

## E

**EBCDIC**

Extended Binary-Coded Decimal Interchange Code. A coded character set consisting of 8-bit coded characters. This standard file format is used primarily on mainframe systems.

**EDIINT**

Refers to the concept of doing EDI over the Internet. In Sterling Connect:Enterprise for UNIX, AS2 is the implementation of EDIINT.

**editor**

A program used to create or manipulate ASCII text. In UNIX, there are several editors available including *ed*, *vi*, and *emacs*.

## **electronic mail**

Often called e-mail, the feature of an operating system allowing computer users to exchange written messages through the computer. The UNIX system mail command provides electronic mail in which the addresses are the login names of users.

## **emacs**

A full-screen text editor. Widely distributed, though not standard on all UNIX implementations.

## **encryption**

An option on the **cmuadd** utility for data security. When this option is used, the data is encoded for protection using an IBM proprietary algorithm, and is stored as a batch in the mailbox.

## **end-of-file (EOF) character**

The character indicating the end of a file.

## **ENQ**

Enquiry. A special character that is part of Bisync communication. The ENQ character is used to obtain a repeat transmission of the response to a message block if the original response was garbled or was not received when expected. ENQ character is also used to bid for the line when using a point-to-point line connection. It also indicates the end of a poll or selection sequence.

## **environment**

The sum of all shell variables that are set individually by the user and are either stored in the profile file or are set manually by the user as needed.

## **environment variable**

A variable supplied by a user to the operating system that describes the operating environment of the process. In Sterling Connect:Enterprise, the environment variables describe the home directory (CMUHOME), and the host name (CMUHOST), for example.

## **/etc**

A UNIX directory containing administrative programs and tables. In Sterling Connect:Enterprise, *\$CMUHOME/etc* directory contains sample startup shell scripts.

## **Ethernet**

One of the most popular LAN communications protocols. See also *Token Ring*.

## **executable file**

A program file that runs simply by typing its name on the command line.



**exit**

To quit a running program. In UNIX, this is technically called terminating a process.

**exit routines**

In Sterling Connect:Enterprise, exit programs are hooks to external user-defined subroutines. When an Exit point is reached, program control is passed to the appropriate subroutine. Any associated data is also passed.

**Exits Daemon (cmuexitd)**

The Sterling Connect:Enterprise process that invokes user-supplied exit programs as various triggering events occur.

**export**

In UNIX, to make environment variables available to other commands. More generally, to send a file or message beyond the immediate system environment. See also *import*.

## F

**FIFO**

First-In-First-Out. The normal method in which a queue is handled. Priority is usually given to the task first entered in the queue.

**file**

A defined set of characters (called bytes) referenced by its file name.

**file names**

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

**file server**

A central computer, normally containing large amounts of memory for storage and connected to all the other computers in its system, that is responsible for connecting and governing the transfer of information through the system.

**filter**

A type of UNIX program that takes input from one file and provides output to the display or another file based on parameters set up by the user. For example, a program that converts EBCDIC-to-ASCII text would be considered a filter.

**flag**

A status message affixed to a data string or batch. In Sterling Connect:Enterprise, a status indicator affixed to a batch in the mailbox. See also *batch status*.

**fork**

A system call that, when invoked by an existing process (parent) causes a new process (child) to be created. See also *child process*, *orphan*, and *parent process*.

**FTP**

File Transfer Protocol. The FTP command used to connect to any other computer on your network running FTP; when connected, FTP can then be used to transfer files to your computer. Can also be used to access files anywhere on the Internet provided you have access to the Internet.

**FTP Daemon (cmuftp)**

The Communications daemon that manages all sessions established with remote sites through the FTP protocol.

**function call**

See *system call*.

**G**

**GENTRAN**

An IBM EDI translation product.

**get**

The FTP command that, in Sterling Connect:Enterprise, enables a remote site to request a specified batch from the mailbox. See also **mget**.

**global key**

A file used to encrypt batches and passwords within Sterling Connect:Enterprise.

## H

### **header**

The beginning area of a file that contains vital information about the file. A mail file contains a header that specifies, among other things, the sender of the message and the route it takes.

### **hexadecimal**

A numbering system with a base of 16; valid numbers use digits 0–9 and characters A–F where A represents decimal 10 and F represents decimal 15.

### **home directory**

The directory the user is placed in after logging on. In Sterling Connect:Enterprise, the home directory is defined by the `CMUHOME` environment variable.

### **host**

The main processing computer at your central site. This is the computer where Sterling Connect:Enterprise is running and where a remote site sends its data batches. Also called host computer.

### **host address**

The name of a specific computer on a network or the name of the entire UNIX system. It can also refer to a specific position away from the network, like the address on a letter.

### **host name**

An alphanumeric string identifying the host computer.

### **HP-UX**

The Hewlett-Packard implementation of the UNIX operating system.

### **HTTP**

Hypertext Transfer Protocol. The client/server protocol used to transfer information on the Web. This is the protocol used to transfer AS2 and WebDAV messages.

### **HTTP Proxy**

The proxy used to send outbound AS2 messages.

## I

### ID

Identification number or text. See also *mailbox ID*.

### import

To get a file or message from beyond the immediate system environment. See also *export*.

### instance key

The key used to encrypt a single batch in a mailbox. The batch instance key is encrypted with the global key and stored in the batch header.

### interactive

A processing method in which each user action causes a response from the program or system. Contrast with *batch processing*.

### 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 allows it to receive and send Internet news and mail.

### Inter-Record Separator (IRS)

A special character used to separate multiple records in a block of data being transmitted over a telecommunications line. Sterling Connect:Enterprise allows either hex 1E or hex 1F as the inter-record separator on Bisync lines, and allows only hex 1E for SNA sessions.

### interrupt

A break in the normal flow of a system or program. Interrupts are initiated by signals generated by hardware indicating that a certain event has happened.

## K

### Kermit

An asynchronous communications protocol.

**kernel**

The core of the UNIX operating system that interacts directly with the computer.

**kill**

A UNIX command that stops a running process.

**L****leased line**

A permanent connection between sites that does not require a dial-up to obtain a communications path. Also referred to as non-switched. Sterling Connect:Enterprise leased line support is point-to-point and therefore allows data to be exchanged only between the local site and a single remote site. Compare with *dial line*.

**library**

A named area on a disk that contains programs and related information.

**line type**

A parameter used to indicate whether a communications line is switched or non-switched (also known as dial or leased, respectively.) See also *dial line* and *leased line*.

**link**

A strategy for saving disk space where several files can share a common file without the need for making copies. In networking, a connection between two items or entities that enables the user to switch easily between the two without having to negotiate the intervening directories.

**local area network (LAN)**

In the PC world, a group of personal computers connected by cable to a central computer (the file server) that distributes applications and files. Novell Netware is an example of a local area network.

**local site**

The physical location of the host computer that runs Sterling Connect:Enterprise. Local users are directly connected to this host computer and directly execute Sterling Connect:Enterprise programs.

## log

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

## Log Daemon (cmulogd)

The Sterling Connect:Enterprise process that records auto connect, remote connect, **cmuadd** and **cmuextract** activity in the *logacct.dat* file and later parses this information for output by **cmureport**.

## logical deletion

A process wherein a batch is flagged as deleted but is not physically removed from the mailbox. A logical deletion is accomplished by either **\$\$DELETE**, **cmudelete**, or the Delete API call. Contrast with *physical deletion*.

## login name

The unique name given to all users on a UNIX system. Usually, a password is also required for access to the system.

## logoff

The process of ending a remote site session with a local site program such as Sterling Connect:Enterprise. A logoff can be a text command or a control function from a remote device.

## logon/login

The process of establishing a session between a remote site and a local site program such as Sterling Connect:Enterprise. A logon may be automatic after a connection is established, or may be entered as a text command or a control function. In Sterling Connect:Enterprise either the remote site or the local site may attempt to initiate the logon process. See also *login name*.

## lp

A UNIX command used to print a file.

# M

## mail

A UNIX command used to send and receive mail from other users.

**mailbox**

The file area used to store electronic mail messages. In Sterling Connect:Enterprise, the area where batches are stored.

**Mailbox Control Definitions File (MCD)**

The file containing the Sterling Connect:Enterprise program parameters used by the Control Daemon at startup. This includes system name, administrator password, security parameters, daemon definitions, and exit enables. This file can be created and modified from the Site Administration user interface provided with Sterling Connect:Enterprise.

**Mailbox Daemon (cmumboxd)**

The Sterling Connect:Enterprise process that manages the reading and writing of batches in the database. It also parses the Mailbox Engine Definitions (MED) file and retains batch status flags for every batch in the database.

**Mailbox Engine Definitions File (MED)**

The file containing parameters used by the Mailbox Daemon that specifies options for system-wide configuration including path information to the mailbox database and its pointer files. This file is created when **cmuinit** is executed to initialize the mailbox.

**mailbox ID**

A 1–8 character name used to identify 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. See also *ID*.

**man**

A UNIX command that displays online manual pages for a specific process. Sterling Connect:Enterprise also contains online man pages that describe local-site commands, API calls, exits, and definition files.

**manual dial**

The host site's method of dialing remote sites to establish a connection on a switched line. With manual dial, an operator at the host site must manually dial the telephone number of the remote site if the connection is initiated by the host site. (If the connection is initiated by the remote site, manual dialing at the host is not used.) Compare with *autodial*.

**metacharacters**

See *special characters*.

## **mget**

The FTP command that, in Sterling Connect:Enterprise, enables a remote site to request multiple batches from the mailbox. See also **get**.

## **modem**

Modulator/demodulator. A device that enables communication over telephone lines between your computer and another computer with a second modem. The modem is responsible for two functions: 1) converting the computer's digital signal into an analog voice signal that can be transmitted across a phone line; 2) receiving a voice signal and reconvertng it into a digital signal that can be understood by the computer.

## **more**

Command in UNIX used to display a file one page at a time.

## **multiplexing**

The ability to accept low-speed data streams from several sources and combine them into one high-speed data stream for transmission to a central site. Multiplexers (MUXs) are the devices that combine these data streams.

## **multiprocessing**

The ability to run more than one program or task at a time; this is one of the great strengths of UNIX.

## **multitasking**

See multiprocessing.

## **multiuser**

The capacity to let more than one user to be active on the system at the same time.

## **MVS**

Multiple Virtual Storage. An IBM mainframe operating system that is one of the other platforms on which Sterling Connect:Mailbox runs.

# **N**

## **NAK**

Negative acknowledgment. It is a special character that is part of Bisync communication. NAK indicates that the previous block was received in error and the receiver is ready to accept a retransmission of the erroneous block. It is also the not ready reply to station selection or line bid.



**network**

Many computers connected by phone lines or direct links so they can share data.

**non-switched line**

See *leased line*.

**O****offline**

The state when Sterling Connect:Enterprise is not actively engaged in sending or receiving batches from local to remote or from remote to local. This is time when various offline utilities can be run that maintain or access data batches in the mailbox. These tasks include local site non-telecommuting tasks like: **cmuadd**, **cmuextract**, **cmudelete**, **cmuerase**, and **cmureport**.

**online**

In general, refers to the state when the computer is actively engaged in some task. In Sterling Connect:Enterprise, the state that allows remote sites to access batches in the mailbox. Sterling Connect:Enterprise is a program run in the host computer that remains active for batch data access until shut down by the local site personnel.

**options**

Characters that modify the default behavior of a command.

**orphan**

A process that runs even though its parent process has been killed.

**P****paging**

A memory-management scheme that divides RAM into 4K segments for more efficient shuffling of data to and from RAM and a hard disk.

**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.

### **parent process**

A process which occurs when a process is split into two the parent and child processes with separate but initially identical text, data, and stack segments. See also *child process*, *fork*, and *orphan*.

### **parent role**

Term used in role-based access to define the set of system permissions from which dependent roles are created. Each dependent role has a subset of the permissions of the parent role that created it and must have at least one parent relationship. See also *role*, *dependent*.

### **parity**

A method of error checking used by asynchronous protocols.

### **parsing**

Logically dividing a command so the user can understand its meaning.

### **passphrase**

A value used to encrypt the global key. The passphrase can contain any character, including spaces.

### **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 the one invoking the system.

### **passwd**

A UNIX command enabling users to change their passwords.

### **pathname**

A sequence of directory names separated by the slash character (/) and ending with the name of the file or directory itself. The path name defines the exact location of the file within the directory structure.

### **peripheral device**

Auxiliary devices under the control of the main computer, used mostly for input, output, and storage functions. Some examples of peripheral devices are terminals, printers, scanners, and disk drives.

**permissions**

A means to define a right to read, write and/or execute a file or directory in the UNIX file system. The rights are specified for the owner of the file, for other members of the owner's group, and for the rest of the world.

**physical deletion**

A process wherein a batch is physically removed from the mailbox by either **cmuerase** or the Erase API call. That batch can be restored by a **cmustatus** command. Compare with *logical deletion*.

**pipe**

A method for enabling standard output from one command to be used as standard input for another command. For example, `ls *.c | lp` would take output for a listing of all files on a disk with the .c extension and print that list out on the printer, where the pipe command is represented by the pipe symbol (`|`).

**pipeline**

A series of filters separated by `|` (the pipe character). The output of each filter becomes the input of the next filter in the line. The last filter in the pipeline writes to its standard output, or may be redirected to a file.

**platform**

A specific operating environment that limits or restricts operation of a particular program. Programs are often identified as platform specific meaning that they will only work within one particular environment. For example, Sterling Connect:Enterprise will only run successfully on a UNIX platform, not on MVS or VSE.

**point-to-point line**

A telecommunications line connection enabling data exchange between two points on the connection, usually the local site and a remote site. Once a dialed connection is established on a switched network, the connection is considered point-to-point. Leased lines where the remote site is a single station are also considered point-to-point.

**polling**

The process whereby data stations are invited to transmit one at a time on a multipoint or a point-to-point connection.

**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.

**process ID**

A unique ID (a number) is generated for each new process created on a UNIX system.

**prompt**

A character used by the shell to indicate that it is waiting for input. In addition, some programs, like ftp, supply their own unique prompts that help the user tell where they are.

**protocol**

A set of rules that determine how a process is accomplished. For example, in telecommunication, a protocol describes how information is transferred across the telephone line. In Sterling Connect:Enterprise, the communications protocols are Async, Bisync, FTP, HTTP.

**put**

The FTP command that, in Sterling Connect:Enterprise, enables a remote site to add a specified batch to the mailbox.

**pwd**

The UNIX command that prints the working, or current, directory.

**Q**

**queue**

A set of tasks awaiting computation that are usually handled in a sequential manner.

**R**

**read**

A UNIX command that reads in user input and places whatever the user types into a shell variable.

**record**

A row in a structured data file. If a user were to create a file containing the names, phone numbers, and salary of every employee, with each employee's information contained in a single row, the row would be called a record.

**record separator**

The character(s) that separate the logical records in a file.

**remote connects**

A term used to indicate that the Sterling Connect:Enterprise session was started by a remote site, either by dialing in or using FTP.

**remote site**

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

**Remote Site Definitions File (RSD)**

The file containing parameters that define how communications are to be conducted with each remote site. For local site users, only a password is supplied in the RSD to enable access local site commands. This file can be created and modified from the Sterling Connect:Enterprise for UNIX Site Administration user interface.

**role**

Term used in role-based access to define a set of system permissions that can be assigned to multiple users. See also *dependent*, *parent role*.

**root directory**

The topmost directory in a file system that contains all other directories and subdirectories. Indicated in all path names as a slash (/).

**routine**

A discrete section of a program to accomplish a set of related tasks.

## S

**schedule**

Term used in the Sterling Connect:Enterprise for UNIX Site Administration user interface to describe the Sterling Connect:Enterprise feature that enables host-initiated data communications to one or more remote sites. The local and remote sites may be connected using manual dial, autodial, or non-switched (leased) lines. The scheduled (auto connect) session may be fully automated by time and day by defining the schedule using the Sterling Connect:Enterprise for UNIX Site

Administration user interface, or controlled with either the `$$CONNECT` or `cmuconnect` commands. Full reporting of schedule (auto connect) activity is available. See also *auto connect*.

## SCP (Secure Copy)

Secure Copy (SCP) is a subprotocol to SSH-1. SCP uses secure shell encryption to protect data transferred across a network or over the internet.

## secondary prompt

A cue displayed at your display by the shell to tell you that the command typed in response to the primary prompt is incomplete. The UNIX shell default secondary prompt is the greater than character (`>>`).

## Secure Sockets Layer

A protocol that provides secure communications with transport protocols, including FTP over TCP/IP and HTTPS. It is an open, non-proprietary Internet protocol that has been widely adopted as standard.

## semaphore

An area in memory that is maintained through a family of system calls that include calls for increasing the value of the semaphore, setting its value, and blocking waiting for its value. This can be thought of as a stop light. It can only be “green” for one “direction” at a time.

## 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.

## Service Interface Daemon (cmusvid)

The service interface daemon manages all communication between the Sterling Connect:Enterprise for UNIX Site Administration user interface and the Sterling Connect:Enterprise for UNIX server.

## 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.

## session ID

A unique session ID (a number) is generated for each Sterling Connect:Enterprise session that is checked into control subsystem (*cmuctld*). A session is defined as any Sterling Connect:Enterprise

subsystem (*cmuexitd*, *cmuasyd*, *cmuftp*, *cmumboxd* and so on) or any of a remote connects serviced by a copy of the communication subsystems (*cmuftp*, *cmuasyd*, *cmubscda*, *cmubscdc*), command line utilities (**cmuadd**, **cmuextract**, and so on). All of these instances has to check in with Sterling Connect:Enterprise control subsystem (*cmuctld*) where an ID will be assigned.

**sh**

A UNIX command used to switch shells.

**shared library**

Object modules and other items that may be shared among several processes at execution time.

**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.

**shell script**

A file containing a series of commands for a UNIX shell.

**shutdown**

A UNIX command used to shut down a UNIX system before powering down. The command **cmushutdown** shuts down Sterling Connect:Enterprise.

**/\*SIGNON**

The leading characters used for logon in Async SPC Emulation mode and Bisync sites in lieu of a \$\$ card.

**smit**

The system administrator's management utility used on AIX systems.

**S/MIME**

A protocol used to encrypt Multipurpose Internet Mail Exchange (MIME) formatted messages.

**Solaris**

The Sun Microsystem implementation of the UNIX operating system.

## **source code**

The uncompiled version of a program written in a language such as C, C++, or Java. The source code must be translated to machine language by a program known as a compiler before the computer can execute the program.

## **SPC Emulation mode**

A mode of operation in which the asynchronous Communications daemon emulates IBM's Software Protocol Converter (SPC) product. Compare with *interactive mode*.

## **special characters**

Characters having special meanings to the shell program and used for common shell functions such as file redirection, piping, background execution, and file name expansion. Special characters include <<, >>, |, &, \*, ? and ].

## **SSH**

Secure Shell (SSH) is a method of secure communications that creates a channel to use a shell on a client computer. Security features included end-to-end encryption, password and public key authentication, and data integrity. Sterling Connect:Enterprise for UNIX allows SSH connections through secure FTP and SCP.

## **SSHFTP Daemon (cmusshftpd)**

The Communications daemon that manages all sessions established with SSH remote sites through the FTP protocol.

## **SSL**

Secure Sockets Layer

## **standard error**

An output stream from a program, normally used to convey error messages.

## **standard input**

The path the data takes: input usually comes from your keyboard or another program. When you specify input to anything but the defaults, you are redirecting the input.

## **standard output**

The path the data takes: output is usually sent to your screen, to a file, or to a printer. When you specify output to anything but the defaults, you are redirecting the output.



**static linking**

The requirements that symbolic references be resolved before run time.

**status line**

A portion of the screen used to provide feedback to the user. Not supported by all UNIX programs.

**Sterling Connect:Mailbox for MVS/VSE**

An 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 offline utilities to manage the batch data storage system on VSAM files called the VSAM Batch Files. Sterling Connect:Mailbox supports the standard protocols including SNA LU1, LU6.2, Bisync, Async and X.25, and provides open connections throughout CICS. Sterling Connect:Mailbox offers real-time, centralized management and control throughout the Sterling Connect:Mailbox network.

**Sterling Connect:Enterprise**

An 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. Sterling Connect:Enterprise for UNIX supports the standard protocols including Bisync, Async, FTP, Secure FTP, HTTP, and Sterling Connect:Direct.

**stop bits**

This option is used by Async protocols. An Async protocol first transmits a start bit, then the character bits, and then the stop bit. A user can configure the number of stop bits transmitted at the end of each character to be one or two bits.

**string**

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

**string variable**

A sequence of characters that can be the value of a shell variable.

**stty**

A UNIX command that enables the user to assign different meanings to a key and adjust the terminal.

**subdirectory**

A directory pointed to by a directory one level above it in the file system organization; also called a *child directory*.

### **subroutine**

A program that defines desired operations and may be used in another program to produce the desired operations.

### **swapping**

Using the hard disk as a slower form of RAM where there is no more RAM available to run programs or store data.

### **switched line**

See *dial line*.

### **sync**

A UNIX command that synchronizes the contents of the RAM file buffers with the disk; usually used in conjunction with the shutdown command. Also, in communications, synchronous conduction of signals across a telephone line.

### **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 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.

### **system call**

A request by an active process for a service performed by the UNIX system kernel, such as I/O, process creation, etc. All system operations are allocated, initiated, monitored, manipulated, and terminated through system calls.

### **Systems Network Architecture (SNA)**

A set of rules, procedures, and structures for a communications network.

## **T**

### **tar**

A UNIX command that saves and restores archives of files on a magnetic tape, flexible disk, or a regular file. It is an abbreviation for tape archive.

**TCP/IP**

Transmission Control Protocol/Internet Protocol. TCP/IP are protocols used to link UNIX to other types of computer systems worldwide, using phone lines.

**telnet**

A UNIX command used for logging into another computer on a UNIX network (like the Internet).

**terminal**

Originally used to describe a dumb computer consisting of little more than a keyboard and a screen that relied on the larger system for its computer power. Now, used to describe any computer used to communicate with a system.

**time-sharing**

A method of operating in which several users share a common computer system seemingly simultaneously. Actually, the computer interacts with each user in sequence; however, the processor's high speed makes it appear to the user that all users are being serviced at the same time.

**/tmp**

A UNIX directory used by the system for temporary storage of working files.

**toggle**

Turning features on or off using the same operation.

**Token Ring**

A LAN communications protocol originated by IBM. See also *Ethernet*.

**trace**

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.

**transparency**

A method of transmitting data over a telecommunications line where in special line control characters embedded in the data are transparent and do not function in their normal capacity as line control characters. Transparency is used when non-text data (such as object modules or other binary data) must be sent over telecommunications lines. Sterling Connect:Enterprise supports Bisync transparency.

## truncation

See *blank truncation*.

## tty

Historically, the abbreviation for a teletype terminal. Today, it is generally used to denote a user terminal.

## turnlines

An optional feature that provides for a limited conversational mode transmission in the Bisync protocol. When the internal command \$TURNLINES\$ is encountered in data being sent to a remote site, the sender temporarily stops sending and issues the proper Bisync protocol to turnaround the line and begin receiving. After all data is received, sending resumes with the record following \$TURNLINES\$.

# U

## UNIX

A general-purpose, multiuser, interactive, time-sharing operating system developed by AT&T Bell Laboratories. The UNIX system enables limited computer resources to be shared by several users and efficiently organizes the user's 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 mailbox. Entry is made in the BATCHID= parameter. See also *BATCHID* and *batch number*.

## user exits

A user-written program called by Sterling Connect:Enterprise at appropriate times during the processing of a transaction. The user-supplied program can alter the standard processing done by Sterling Connect:Enterprise. User Exits can be supplied to examine all input data from a remote site, to examine output data to a remote site, to provide unique security processing, or to examine and alter data in Sterling Connect:Enterprise commands as well as to automate the system.

## userid

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

## V

### **vi**

A text editor packaged with most UNIX systems.

### **VSE**

Virtual Storage Extended. One of the oldest and most established IBM mainframe operating systems.

## W

### **WACK**

Wait-before-Transmit Positive Acknowledgment. A special character that is part of Bisync communication. WACK allows a receiving station to indicate a temporarily not ready to receive condition to the transmitting station. It can be sent as a response to a text or heading block, selection sequence (multipoint), line bid (point-to-point with contention) or an ID (identification) line bid sequence (switched network). WACK is a positive acknowledgment to the received data block to or selection.

### **who**

A UNIX command that displays other users logged on the system.

### **wildcard**

Special characters within a file name that tells the shell to search for all files with similar file names: \*r, for example, would tell the shell to return all files ending with the letter *r*.

### **workstation**

A powerful, networked, single-user computer.

### **write**

A UNIX command that lets you send instant messages to other users logged into the system.

### **WebDAV**

The Web-based Distributed Authoring and Versioning (WebDAV) protocol is a set of extensions that work within the HTTP protocol. These extensions allow you to manage and edit data that is located on remote Web servers.

## X

### **XMODEM**

An asynchronous communications protocol.

## Y

### **YMODEM**

An asynchronous communications protocol.

## Z

### **ZMODEM**

An asynchronous communications protocol.

## A

administrative ID 43

API error codes 247

Applicability Standard 2

- background information 177
- defined 268

AS2 35

- Configuring After Installation 181
- defined 268
- prerequisites for implementing 177
- sending and receiving data illustrated 177

AS2 contract

- digital signature information worksheet 185
- encrypted messages information worksheet 185
- identity information worksheet 183
- information required to create 183
- message options worksheet 186
- SSL information worksheet 184

AS2 Implementation 177

AS2 port

- configuring for incoming messages 182
- worksheet 182

as2report utility

- defined 163
- parameters 163

ASCIIToEBCDIC 265

Authentication Server Daemon 75

Auto Connect

- status codes 249

auto connect

- detail report 156
- summary report 158

auto connect daemon 78

## B

batch

- ID 13

batch encryption 129

Bisync daemon

- cmubscdc 96

bulk file

- applying password policy 121

## C

ceinstall installation program 24, 51

cereport

- configuring 42

cereport function

- description 14

certificate and algorithm requirements

- defining AS2 contracts 185

ceukey 127, 130

ceupassadm

- applying password flags 121
- creating password policy 119
- displaying policy file contents 121
- forcing password change 120
- function 116
- parameters 117

ceupassencrypt 127, 133

ceupassrpt

- function 116
- generating password policy reports 122

ceupasswd

- changing user password 124
- function 116
- parameters 125

ceushutdown 101, 102

- example 101, 102
- parameters 101, 103

CEUSIPSKEYLOCATION 238

ceustartup 69, 71

- modifying 72

## Index

- ceustartup.trace 71
    - modifying 72
  - cmuacd 72, 78, 79
    - parameters 80
  - cmuasyd 85
    - parameters 86
  - cmuauthd 75, 269
  - cmubscda 72, 94
    - parameters 95
  - cmubscdc 72
    - Bisync daemon 96
    - description 96
  - cmucheckcfg 134, 145
  - cmuctld 72, 73
  - cmuediintd 72, 274
    - communications daemon 99
  - cmuexitd 72, 81
    - parameters 81
  - cmufixup 134
    - examples 146
  - cmuftpd 23, 72, 87
    - parameters 88
  - CMUHOME 58, 59
    - customizing high availability 34
  - CMUHOST 59
  - cmuhttpd 72, 275
    - communications daemon 98
  - cmuinit 136
    - example 146, 147
  - cmulogd 72, 78, 85
    - log daemon 88
    - parameters 78
  - cmumboxd 72, 76
    - parameters 76
  - CMUPASWD 59
  - CMUPOINT 59
    - customizing high availability 34
  - cmurebuild 137
  - cmureport 88, 149
  - cmusipskey 237
  - cmusshftpd 92
    - parameters 92
  - cmusshkey 131
  - cmusvid 82, 294
  - CMUSER
    - customizing high availability 34
  - command line utilities 78
    - cmureport 88
  - Communications protocols 14
  - configuration
    - locating problems 134
  - configuration file
    - password administration 114
  - Configure Sterling Connect Enterprise Agents and Cereport 42
  - Control daemon 28
  - control file records
    - correcting 134
  - Creating the user ID 23
- ## D
- daemons 72
    - async daemon 85
    - auto connect daemon 79
    - Bisync sub-system daemon 94, 96
    - control daemon 73
    - exit daemon 81
    - FTP daemon 87, 92
    - log daemon 78, 79, 85, 88
    - mailbox daemon 76
  - data collection, definition 11
  - data transmission, definition 12
  - debug tracing 94
  - Displaying and Printing Reports 151
  - Displaying Pipe-Delimited Reports 152, 163
- ## E
- EBCDICtoASCII 265
  - EDIINT
    - defined 279
    - implemented with AS2 279



encrypt.cfg 129

encrypted messages worksheet  
 defining AS2 contract 185

encryption  
 batch 127, 129  
 password 127

encrypted messages worksheet  
 defining AS2 contract 186

environment variables  
 exporting 57

error messages 239, 240  
 API 247  
 Auto Connect status codes 249  
 Remote Connect status codes 251  
 utility exit codes 253

EURO 266

exit codes  
 utilities 253

## F

Firewall  
 Running Protocol Daemon Outside the 205

ftp 23, 87

ftpd 23, 87

## G

Generating Reports 151

global key 127

## H

high availability  
 installation 34

host name 43

HTTP 283  
 use with AS2 177

HTTP daemon  
 parameters defined 98

HTTP proxy  
 worksheet 183

HTTP proxy servers  
 sending AS2 messages 183

## I

identity information  
 defining AS2 contract 184

Installation  
 CD contents 16  
 creating the user ID 23  
 preparation 21

interval 44

## M

mailbox  
 initializing 136

mailbox control files  
 reconstructing 137

Mailbox ID 13

MANPATH 59

Message encryption 237

message options worksheet  
 defining AS2 contract 186

messages  
 error 239

modifying 91

MQ Agent  
 configuring 42

MQSeries 14

multilevel role-based access  
 role dependencies 107

multilevel role-based system  
 creating 107

## O

offline utilities log  
 report 162

## P

parameters  
 password administration configuration file 115

password administration  
 authentication log file 125  
 overview 113  
 utilities 116

password administration files  
 illustration 113

password configuration file  
 parameters 115

password encryption 127, 133

Password Policy  
 Creating 119

password policy  
 creating 119

password policy file  
 RSD policy file 115  
 security 116

PATH 59

permissions defined 108

policy file  
 creating and applying 117  
 defined 115

policy files  
 common parameters 119  
 types 115

port number 43

post-installation 57

Protocol Daemon Outside the Firewall 205

**Q**

queued auto connect  
 report 161

**R**

Remote Connect  
 status codes 251

remote connect  
 detail report 159  
 summary report 160

Remote Daemons  
 Installing 206

remote ID 43

remote ID password 43

report utility  
 as2report 163

Reports  
 Displaying and Printing 151  
 Displaying Pipe-Delimited 152, 163  
 Generating 151

reports  
 AS2 protocol activity 163  
 auto connect detail report 156  
 auto connect summary report 158  
 displaying 151  
 offline utilities log 162  
 printing 151  
 queued auto connect 161  
 remote connect detail report 159  
 remote connect summary report 160

rftp 87

role permissions 110

role-based access 14  
 multilevel design 107  
 overview 105  
 single-level design 105

RSD policy  
 parameters 119

RSD policy file  
 defined 116

RTICDIR 59

**S**

Secure FTP 30, 56

Service Daemon 82

Service daemon 23, 29

servlet engine 21

Shutting Down Sterling Connect  
 Enterprise 101  
 Enterprise Base 102

Signon Banner 91

single-level access system  
 creating 106

single-level role-based access  
 role dependencies 105

SIPS encryption 237

Site Administration user interface 66

SSH 32, 173  
   Configuring 173

SSH daemon 92

SSL worksheet  
   defining AS2 contract 184

status codes  
   Auto Connect 249  
   Remote Connect 251

Sterling B2B Integrator 14

Sterling Connect:Enterprise  
   command line utilities  
     cmureport 88  
   communications protocols 14  
   daemons  
     communications daemons 72  
   description 11  
   features 14  
   File Agent 14  
   host name 43  
   installation  
     CD contents 16  
     creating the user ID 23  
     preparation 21  
   overview 11, 14  
   port number 43  
   remote ID 43  
   remote ID password 43

Sterling Connect:Enterprise for UNIX Site  
   Administration user interface 14

subprocess 44

superuser ID 43

SYNCCable+ device 96

system policy file  
   system password policy 115

system resources 108

## T

testing the installation 59

The 96

Timeout Values 66

translate table format 265

## U

upgrading 133

URL  
   defining for HTTP proxy server 183

User ID 23

utilities exit codes 253

## V

VSAM batch files  
   definition 12

## W

wait cycle 44

Web server 21



---

# 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](http://www.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](http://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.