Connect:Enterprise UNIX®

Installation and Administration Guide

Version 2.4

Sterling Commerce
An IBM Company

Connect:Enterprise UNIX Installation and Administration Guide
Version 2.4

First Edition

Sterling Commerce, Inc.

4600 Lakehurst Court Dublin, OH 43016-2000 *
614/793-7000

Contents

Chapter 1

About Connect:Enterprise UNIX

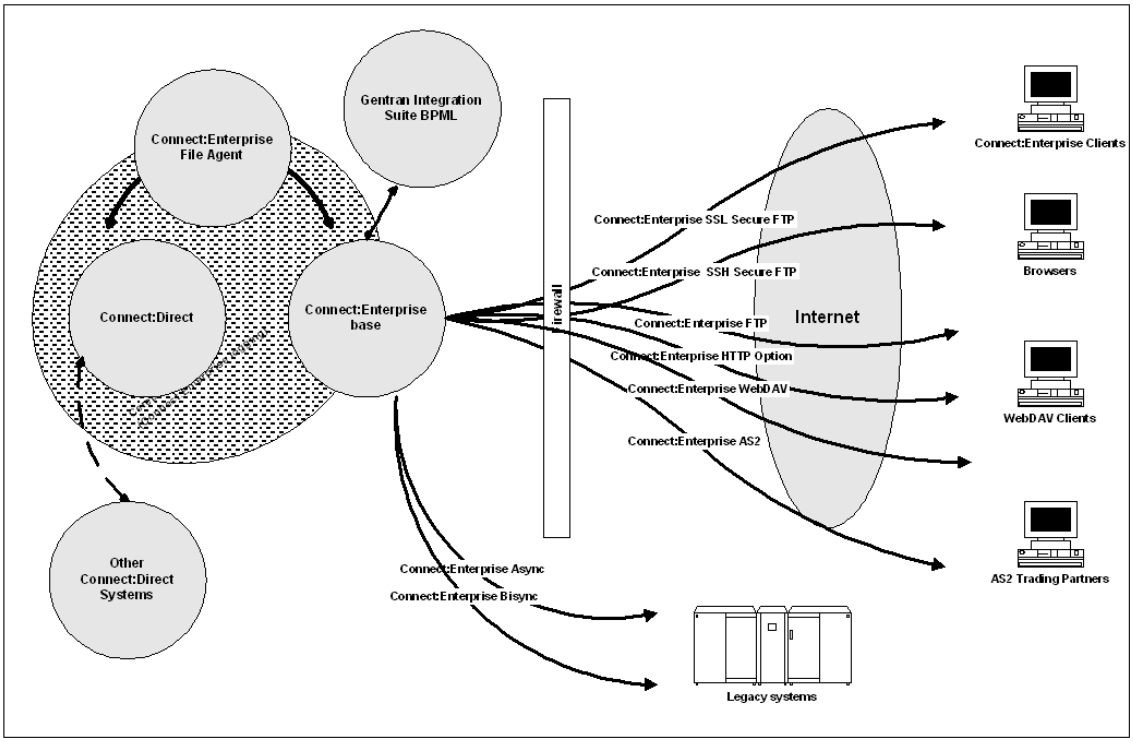
Connect:Enterprise is an online data communications system developed by Sterling Commerce for use with large networks within a UNIX environment. Connect:Enterprise enables the exchange of information between and within companies, including unattended, automatic data collection and distribution.

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

Refer to the *Connect:Enterprise UNIX Version 2.4.00 Release Notes* for release-specific information.

Transmitting and Collecting Data

Connect:Enterprise 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 Connect:Enterprise administrator assigns mailboxes and controls access to the mailboxes through Connect:Enterprise UNIX user IDs and passwords. After a communications session is established between Connect:Enterprise 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 Connect:Enterprise UNIX repository can be initiated from an FTP or SSHFTP client, an Async or Bisync remote, a browser using the Connect:Enterprise HTTP Option, a GIS business process, or an AS2 trading partner. The following figures shows the communications flow between the Connect:Enterprise UNIX server installed in the trusted zone and its remote trading partners.



Connect:Enterprise UNIX collects data files from remote sites for a central host site. For example, 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.

Connect:Enterprise 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.

Connect:Enterprise 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.

Connect:Enterprise UNIX Terminology

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

Term	Connect:Enterprise UNIX Definition	Synonym
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	Connect:Enterprise 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 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	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. 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).	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 Connect:Enterprise UNIX repository to distribute or collect data.	
Remote connect	Communications session with the Connect:Enterprise UNIX repository initiated by a remote site.	

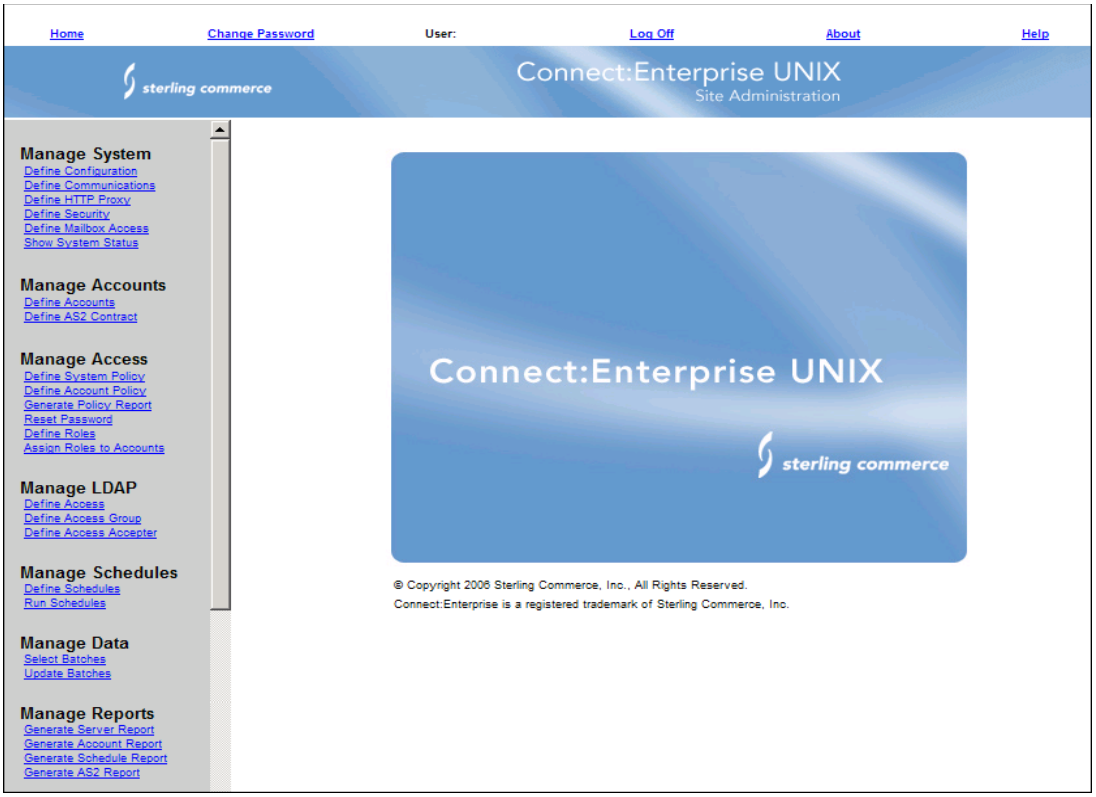
Connect:Enterprise Features

Connect:Enterprise UNIX has the following features:

- Firewall navigation support allows controlled access to a 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 SFTP and SCP, HTTP, asynchronous, bisynchronous, Connect:Direct, and Gentran Integration Suite (GIS) 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 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 Connect:Enterprise repository and the IBM MQSeries product.
- The Connect:Enterprise Site Administration user interface allows you to administer Connect:Enterprise base from a browser.
- Role-based access allows you to specify sets of permissions and assign these permission sets to different users.

Connect:Enterprise UNIX Site Administration User Interface

The Connect:Enterprise UNIX Site 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 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 Connect:Enterprise system.
Access	Enables you to define and assign roles for users of the Connect:Enterprise Site Administration interface, and create and assign password policies to users.

Resource	Description
LDAP	Enables you to configure the communications between 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 Connect:Enterprise 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 Connect:Enterprise UNIX Site Administration user interface. See also *Setting Up the Connect:Enterprise UNIX Site Administration User Interface* on page 94 for instructions on configuring the Connect:Enterprise UNIX Site Administration user interface.

Connect:Enterprise Software

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

Component	Description	Installation Reference
Connect:Enterprise UNIX Secure FTP or Connect:Enterprise UNIX FTP Connect:Enterprise UNIX AS2	Provides the Connect:Enterprise UNIX software with Secure FTP capability, AS2 capability, or without Secure FTP or AS2 capability, Connect:Enterprise File Agent.	*Connect:Enterprise UNIX Installation and Administration Guide* Connect:Enterprise Integration Tools User's Guide (File Agent)
Connect:Direct UNIX.	Provides Connect:Direct UNIX software.	*Connect:Direct UNIX Getting Started Guide*
Connect:Direct Browser User Interface	Enables you to create, submit, and monitor Connect:Direct Processes from an Internet browser and perform some Connect:Direct system administration tasks.	Connect:Direct Browser User Interface Readme file

Component	Description	Installation Reference
Sterling Commerce Certificate Wizard	Packaged only with Connect:Enterprise UNIX Secure FTP. Automates creating certificate signing requests.	Sterling Commerce Certificate Wizard ReadMe file

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

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

Connect:Enterprise UNIX Documentation

See *Connect:Enterprise UNIX Version 2.4.00 Release Notes* for a complete list of the product documentation.

About This Guide

Connect:Enterprise UNIX Installation and Administration Guide is for programmers and network operations staff who install, configure, andmaintain the Connect:Enterprise UNIX version 2.4 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 perfrom the tasks documented in this guide:

Task	For More Information, See
Installing Connect:Enterprise UNIX	Chapter 2, *Installing Connect:Enterprise UNIX*
Installing Connect:Enterprise base	Chapter 2, *Installing Connect:Enterprise UNIX*
Installing individual components of Connect:Enterprise UNIX	Chapter 2, *Installing Connect:Enterprise UNIX*
Upgrading from a previous version of Connect:Enterprise or Connect:Mailbox	Chapter 3, *Upgrading Connect:Enterprise UNIX*
Exporting environment variables	Chapter 4, *Post-Installation Tasks*
Installing the license management key file	Chapter 4, *Post-Installation Tasks*
Testing the installation	Chapter 4, *Post-Installation Tasks*
Setting up the Connect:Enterprise UNIX Site Administration user interface	Chapter 4, *Post-Installation Tasks*
Starting and stopping Connect:Enterprise UNIX	*Chapter 5, Starting and Stopping Connect:Enterprise*
Designing a role-based access system	Chapter 6, *Role-Based Access*
Defining and applying password policies, changing user password, and generating reports on RSD policy files	Chapter 7, *Password Administration*
Issuing administrator commands	*Chapter 8, Administrator Commands*
Generating reports	*Chapter 9, Generating Reports*
Installing Secure FTP	Chapter 10, *Configuring Secure FTP*
Implementing SSH FTP	Chapter 11, *Configuring SSHFTP Protocol*
Implementing AS2	Chapter 12, *Configuring AS2*
Implementing WebDAV	Chapter 13, *Configuring WebDAV Protocol*
Implementing External Authentication	Chapter 14, *Configuring the External Authentication Service*
Configuring Remote Daemons	Chapter 15, *Running Protocol Daemons on Remote Servers*
Implementing Connect:Enterprise in a high-availability environment	Chapter 16, *Configuring High Availability*
Implementing SIPS Encryption	Chapter 17, *Encrypting Internal Product Communications*
Troubleshooting problems	*Appendix A, Error Messages*

Chapter 2

Installing Connect:Enterprise UNIX

This chapter provides information about the Connect:Enterprise 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 Connect:Enterprise UNIX components, installing Connect:Enterprise UNIX base, installing Connect:Direct UNIX, and configuring Connect:Enterprise UNIX agents and cereport.

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

Before You Begin

Perform the following tasks before you install Connect:Enterprise.

1. If you plan to use a third-party Web server to run the 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 *Connect:Enterprise 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	◆ Installs Connect:Enterprise UNIX ◆ Configures Secure FTP, SSH, High Availability, AS2, and HTTP server, as required for your system ◆ Installs File Agent, MQ Agent, and cereport	◆ *Starting the Installation Script* on page 22 ◆ *Installing All Connect:Enterprise UNIX Components* on page 23 ◆ *Installing Connect:Enterprise UNIX Base on page 24*
Install the base product	◆ Installs Connect:Enterprise UNIX ◆ Configures SSH, Secure FTP, High Availability, AS2, and HTTP server, as required for your system	◆ *Starting the Installation Script* on page 22 ◆ *Installing Connect:Enterprise UNIX Base on page 24*
Upgrade the base product	Upgrades your installation from an earlier version of Connect:Mailbox or Connect:Enterprise	Refer to *Chapter 3, Upgrading Connect:Enterprise UNIX*.
Install or upgrade remote daemons	Installs or upgrades a protocol daemon on a remote system such as a DMZ machine.	Refer to *Installing Connect:Enterprise Remote Daemons on page 38*.
Configure agents and cereport utility	Configures File Agent, MQ Agent, and cereport	◆ *Starting the Installation Script* on page 22 ◆ *Configuring Connect:Enterprise File Agent, MQ Agent, and cereport on page 41*

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	*Configuring Secure FTP* on page 191
SSHFTP	*Configuring Connect:Enterprise SSHFTP Server* on page 199
AS2	*Configuring Connect:Enterprise UNIX for AS2* on page 207
High Availability	*Installing Connect:Enterprise High-Availability Scripts* on page 241

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 Connect:Enterprise to reside.

7. Identify the port number for the Control daemon. This is the TCP/IP port number the Connect:Enterprise Control daemon monitors for connection requests from the other 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 Connect:Enterprise Service daemon monitors for requests from the Connect:Enterprise Site Administration user interface (the installation procedure provides a default value).
9. Verify that Java Developer's Kit (JDK) is installed on the host.
10. 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.
11. 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 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 Connect:Enterprise from the root account.

The 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 Connect:Enterprise UNIX installation script, select the installation option, and specify the destination directory. You cannot install Connect:Enterprise 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 Connect:Enterprise installation from an ESD portal, navigate to the location of the **ceinstall** script.
   - If you acquired your Connect:Enterprise installation on a CD-ROM, mount the Connect:Enterprise UNIX CD-ROM.
2. At the UNIX prompt, type:

```
ceinstall
```

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

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
Installation Procedure

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

Sterling Commerce, Inc.(TM) and Connect:Enterprise(TM) UNIX(TM) are trademarks
of Sterling Commerce, Inc. in the U.S.A. and other countries.

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/).
Media location:
```

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 Connect:Enterprise UNIX components
  (2) Install or upgrade Connect:Enterprise UNIX base
  (3) Install or Upgrade Connect:Enterprise UNIX remote daemons.
  (4) Configure the Connect:Enterprise UNIX 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 Connect:Enterprise UNIX Components* on page 23
   - *Installing Connect:Enterprise UNIX Base on page 24*
   - *Installing Connect:Enterprise Remote Daemons* on page 38
   - *Configuring Connect:Enterprise File Agent, MQ Agent, and cereport on page 41*

Installing All Connect:Enterprise UNIX Components

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

1. Complete the procedure in *Starting the Installation Script* on page 22.
2. When the Installation menu is displayed, type **1** and press **Enter**. The following message is displayed:

```
Connect:Enterprise UNIX 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 Connect:Enterprise UNIX 2.4.00.
You can use $HOME to shorten the name: [$HOME/ceunix]
```

4. Type the complete path to the directory where you want to install Connect:Enterprise 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 Connect:Enterprise UNIX Base on page 24*.

Installing Connect:Enterprise UNIX Base

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

1. Complete the procedure in *Starting the Installation Script* on page 22.
2. Type **2** to specify the installation and press **Enter**. The following message is displayed:

```
Connect:Enterprise UNIX base Version 2.4.nn will be installed on 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 Connect:Enterprise UNIX Version 2.4.00.
You can use $HOME/ceunix to shorten the name:
[/install_directory]
```

4. Type the complete path to the directory where you want to install Connect:Enterprise 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
version Version 2.4.nn Installation Procedure

You are beginning the Connect:Enterprise UNIX Installation Procedure.
You have specified the following directory (called the destination directory)
/sci/users/user1/ceunix
where the Connect:Enterprise UNIX files will be stored.

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

Sterling Commerce, Inc.(TM) and Connect:Enterprise(TM) are
trademarks of Sterling Commerce, Inc. in the U.S.A. and other countries.

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 Connect:Enterprise UNIX Version 2.4.nn

Approximately 104000 kbytes of disk space is required
to install Connect:Enterprise UNIX.
(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          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   99158   41445   71% /
/dev/vg00/lvol1     295024   35632  229888   13% /stand
/dev/vg00/lvol8    1126400  696199  403450   63% /var
/dev/vg00/lvol7    1536000  989927  511984   66% /usr
/dev/vg00/lvol4      65536   12821   49463   21% /tmp
/dev/vg00/lvol10   2048000 1788727  243376   88% /sci
/dev/vg00/lvol9    1536000  442042 1025591   30% /qa
/dev/vg00/lvol6    1536000  825558  666092   55% /opt
/dev/vg00/lvol5     524288    1238  490364    0% /home
/dev/vg00/lvol11   5632000 2214201 3207635   41% /export1
/dev/datavg/data   34930688 17105080 17686960   49% /data

You have ##### kbytes of disk space available to you,
which is more than the required 104000 kbytes.

Do you want to continue? [Y/n]
```

8. Press **Enter** to continue if the disk space is sufficient. 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 customize Connect:Enterprise UNIX.
```

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

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
version Version 2.4.nn Customization

The customization procedure sets up the Connect:Enterprise UNIX
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]
```

10. Type the system host name or accept the default and press **Enter** to begin the customization procedure to create the 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 (ksh, bsh, csh) in
/sci/users/user1/ceunix21/etc/ ....

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

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

12. Type the TCP/IP port number that the Connect:Enterprise Control daemon monitors for connection requests from other 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 Connect:Enterprise Web Services daemon monitors for connection requests from the 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....

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 Connect:Enterprise FTP daemon monitors for connection requests from remote sites, or press **Enter** to accept the default.
15. 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 Connect:Enterprise.

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

```
Please enter the Connect:Enterprise UNIX RSD password [userID]:
```

16. Type the password associated with userID and press **Enter**.
17. If you purchased the external authentication option, you are prompted with the following:

```
Do you want to configure external authentication? [y|N]
```

Type **y** and press **Enter** to configure external authentication.

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

18. You are prompted with the following:

```
Enter external authentication non-secure port number: [61365]
```

Type a port number or accept the default and press **Enter**.

Customizing Connect:Enteprise UNIX

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

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

The customization scipt 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	*Configuring Secure FTP* on page 191
SSHFTP	*Configuring Connect:Enterprise SSHFTP Server* on page 199
AS2	*Configuring Connect:Enterprise UNIX for AS2* on page 207
High Availability	*Installing Connect:Enterprise High-Availability Scripts* on page 241
HTTP (WebDAV)	For more information on configuring WebDAV, see the Site Administration User Interface Help.

Setting Up Secure FTP

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

```
This product requires the use of an X.509 certificate.
You can generate a Certificate Signing Request (CSR) and verify
Key/Cert 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:

```
** Connect:Enterprise Secure FTP with SSL Setup Script **
Enter the path for your new private key: ["/usr/mailbox/ceunix/spd/privkey.txt"]
```

2. Type the complete path where you want to place your new private key, and press **Enter**. The following prompt is displayed:

```
Enter the path for your new Certificate Signing Request, a.k.a., CSR:
["/usr/mailbox/ceunix/spd/csr.txt"]
```

3. Type the complete path where you want to place your new Certificate Signing Request (CSR) and press **Enter**. The following prompt is displayed:

```
Would you like to encrypt your private key with a password? [y|N]:
```

Note: The default for this prompt is **No**.

4. Type **y** for the additional security of encrypting your private key with a password. Type **n** (or press **Enter**) if you do not want to use a password.

Note: If you type **y**, you are prompted to enter and verify a password. Your private key password can be up to 256 characters.

The following prompt is displayed:

```
Enter length (in bits) of your private key (512-2048): [1024]
```

5. Type the length of your private key in bits and press **Enter**. It can be any length between 512 and 2048 bits. The default is 1024.

   The utility to generate an SSL Certificate Signing Request starts, using the files specified in the previous steps. A screen, similar to the following, is displayed:

```
**** running 'cmusslgencsr -k /usr/mailbox/ceunix/spd/privkey.txt
-c /usr/mailbox/ceunix/spd/csr.txt -l 1024 '
**
# Connect:Enterprise UNIX Private Key and CSR Generation Utility #
# Setting Up #
# Generating RSA key pair [1024-bit]
#Using default password 'password'
# File '/usr/mailbox/ceunix/spd/privkey.txt' contains your encrypted private
key #
#Generating Certificate Signing Request #
2 Letter Country Code (max 2 characters):
```

6. Type your two-letter country code and press **Enter**. The following prompt is displayed:

```
State/Province (max 128 characters):
```

7. Type the name of your state or province and press **Enter**. The following prompt is displayed:

```
City/Locality (max 128 characters):
```

8. Type the name of your city or locality and press **Enter**. The following prompt is displayed:

```
Organization Name (max 128 characters):
```

9. Type the name of your organization and press **Enter**. The following prompt is displayed:

```
Organizational Unit (max 128 characters):
```

10. Type the name of your organizational unit and press **Enter**. The following prompt is displayed:

```
Common Name (server host name) (max 128 characters):
```

11. Type the host name of your server and press **Enter**.

    A screen, similar to the following, is displayed:

```
# You may submit file 'usr/mailbox/ceunix/spd/csr.txt' to your CA to request a
certificate #

Private key and CSR generated successfully.  You may now submit your CSR to a CA,
from which you should then receive a certificate.  You should then concatenate the
certificate with your private key to create your Key/Cert file.
```

Note: For instructions on requesting, distributing, and installing certificates, refer to Chapter 10, *Configuring Secure FTP*.

The following prompt is displayed:

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

12. 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]
```

13. 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.

    The next screen allows you to complete the Secure FTP installation.

```
Enter the FULL path where you will place your Key/Cert file:
["usr/mailbox/ceunix/spd/keycert.txt"]
```

14. Type the path to the directory where you would like to create a placeholder for the Key/Cert file. See Chapter 10, *Configuring Secure FTP*, for a description of the Key/Cert file.

    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* **cmusshcust** script.

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

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

2. Type the TCP/IP port number that the 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 hit 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/users/user01/ceunix2200s/ssh/system/host_key
Your public key is being saved in:
 /data/users/user01/ceunix2200s/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.

Would you like to build a keypair for the samp_ssh example? [Y|n
```

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 33. 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/users/user01/ceunix2200s/ssh/users/samp_ssh/id_rsa
   Your public key is being saved in:
    /data/users/user01/ceunix2200s/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/ceunix21
was detected to be the location of Connect:Enterprise Secure FTP.

Is this correct? [Y|n]
```

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

```
================================================================================
Sterling Commerce, Inc., (TM) Connect:Enterprise UNIX (TM)
Version n.n High-Availability Package Installation Procedure

The Connect:Enterprise 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 Connect:Enterprise 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) Unix(TM)
version n.n.nn Customization

This customization procedure sets up AS2 for Connect:Enterprise 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**. The following prompt is displayed:

```
Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version x.x.xx     at /usr/java/jdkx.x.xx/bin/java
2 = version x.x.xx     at /usr/java/jdkx.x.xx/jre/bin/java
Select [0-2]:
```

3. Select the Java version to use and press **Enter**. The installation proceeds and the script returns to the customization script.

Setting Up the HTTP Server

Connect:Enterprise 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 tp 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:

```
Enter port number for the HTTP Services daemon listener [8002]
```

2. 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**.

   If you did not select to configure AS2, the following prompt is displayed:

```
Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version x.x.xx     at /usr/java/jdkx.x.xx/bin/java
2 = version x.x.xx     at /usr/java/jdkx.x.xx/jre/bin/java
Select [0-2]:
```

3. Select the Java version to use and press **Enter**. The following prompt is displayed:

```
Created script: /sci/users/user01/ceunix2200s/javalib/cmuadmind
Updating ceuadmin's system.properties file with:
   addr = hostname
   port = port#
Found jar at /usr/j2se/bin/jar
adding: property/(in = 0) (out= 0)(stored 0%)
adding: property/system.properties(in = 178) (out= 76)(deflated 57%)

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

For WebDAV access use:
http://hostname:port#/ceuadmin/jsp/index.jsp
Hit enter to continue.
```

4. The installation proceeds and the script returns to the installation menu.

Completing the Installation

After all components are installed, the customization script continues with the following prompt:

```
....Creating ceustartup script....

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

....Creating ceushutdown script....
```

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

```
==========================================================================
To Start Connect:Enterprise UNIX, you must install the license management key
included with your shipment. The key shipped
with the product is a temporary key and must be replaced with a permanent
key that you request from your Sterling Commerce account representative.
The license management key must be installed and renamed to
/$CMUHOME/etc/license.key.
Please refer to the Installation and Administration Guide for instructions.
==========================================================================

Please press ENTER to continue...
```

2. Press **Enter** to continue the installation. The following prompt is displayed:

```
Connect:Enterprise UNIX configuration completed.

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

export CMUHOME=/$CMUHOME/ceunix2
export CMUHOST=cmuhostname
export CMUPORT=xxxx
export PATH=$PATH:$CMUHOME/etc:$CMUHOME/os/bin
export LD_LIBRARY_PATH=${CMUHOME}/os/lib
export LIBPATH=${CMUHOME}/os/lib
export SHLIB_PATH=${CMUHOME}/os/lib


You can set the environment variables later by executing
/$CMUHOME/etc/profile
at shell prompt

OR

incorporate $CMUHOME/etc/profile into
your environment.


==========================================================================

Please press ENTER to continue...
```

3. Press **Enter** to continue the installation. The following prompt is displayed:

```
================================================================
Connect:Enterprise UNIX configuration completed.

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

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

Connect:Enterprise UNIX base version 2.4.00 install successful.

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

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

Installing Connect:Enterprise Remote Daemons

Connect:Enteprise 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 22.
2. With the Installation menu displayed, type **3,** and press **Enter**. The following prompt is displayed:

```
Selected Connect:Enterprise UNIX 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 Connect:Enterprise UNIX 2.4.00.
You can use $HOME/ceunix to shorten the name:
[$CMUHOME/remotehost
```

4. Type the host name where you want to install the daemons and press **Enter**. After the binaries are installed, the following prompt is displayed:

```
Connect:Enterprise UNIX has been successfully installed.

Press ENTER to start the customization process.
```

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

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
version 2.4.00  Customization

The customization procedure sets up the Connect:Enterprise UNIX
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.
```

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

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

7. Type the name of the host where the 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 Connect:Enterprise core daemons are running.

The following prompt is displayed:

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

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

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

Enter port number for the Control daemon listener: [8000]9999
```

9. Type the port number of the control daemon that resides on the host specified in step 7 on page 39 and press **Enter**.
10. The following prompt is displayed:

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

11. 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]
```

12. Type the listener port number of the FTP daemon and press **Enter**. If you have 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]
```

13. If want to set up SSL, type **y** and press **Enter**. Refer to *Setting Up Secure FTP* on page 28.
14. After you set up SSL, the following prompt is displayed:

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

15. To install the SSH daemon on the remote server, type **y** and press **Enter**. Refer to *Setting Up SSH* on page 31 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]
```

16. If want to set up the AS2 HTTP daemon, type **y** and press **Enter**. Refer to *Setting Up AS2* on page 34. After you set up the AS2 HTTP daemon, The following prompt is displayed:

```
This release of C:E UNIX contains an HTTP Server (ceuadmind)
that supports the C:E UNIX Browser Interface (ceuadmin).
Note: A java run-time is required for this option.


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

17. To install the HTTP daemon to serve WebDAV requests, type **y** and press **Enter**. Refer to *Setting Up the HTTP Server* on page 35 for information on setting up the HTTP daemon. After you set up the HTTP daemon, refer to *Completing the Installation* on page 36.
18. Refer to *Running Protocol Daemons on Remote Servers* on page 231 for additional information.

Installing Connect:Direct UNIX

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

Configuring 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 22.
2. With the Installation menu displayed, type **4,** and press **Enter**. The following prompt is displayed:

```
The Connect:Enterprise UNIX n.n.nn 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 Connect:Enterrise UNIX home directory [/data/ceunix]:
```

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 Connect;Enterprise UNIX API connection information below.
Enter Connect:Enterprise 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 Connect:Enterprise API port number [8000]:
```

4. Type the API port number that corresponds to the control port number entered during the 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 Connect:Enterprise API RemoteID [username]:
```

5. Type the Connect:Enterprise API remote ID and press **Enter**. This is the Connect:Enterprise user ID that the File Agent uses as the originating mailbox remote for all batches added to

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

6. Type the 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 Connect:Enterprise superuser ID. This is the administrative ID used by the administrator for Connect:Enterprise. This prevents internal security in Connect:Enterprise from interfering with the operation of the File Agent.

The following prompt is displayed.

```
Warning: The 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:

```
Connect:Enterprise UNIX API Host:             hostname
Connect:Enterprise UNIX API Port:             portnumber
Connect:Enterprise UNIX API User Name:        user01
Connect:Enterprise 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:                          ##
Connect:Enterprise UNIX API Host:          hostname
Connect:Enterprise UNIX API Port:          portnumber
Connect:Enterprise UNIX API User Name:     username
Connect:Enterprise 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 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
setup the MQ series agents

If you do have the MQ series libraries installed now, you may choose 'yes' at the
prompt in order to setup 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:

```
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.

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
cereport Customization

The customization procedure will create or override cereport script in directory
/$CMUHOME/etc

To abort the process, enter Control-C.

================================================================================

Press ENTER to continue. . .
```

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

```
Using Java Runtime "/usr/java1.4/bin/java" to configure Cereport

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

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

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

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

```
Enter the FULL path name of the Connect:Enterprise base log
directory:[$CMUHOME/log]
```

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

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

5. The following is displayed:

```
The script /$CMUHOME/etccereport has been created!
To execute the Conenct:Enterprise reporting tool, run cereport at the shell
prompt.
```

6. Press **Enter** to return to the installation menu. To exit the installation menu, type **5** and press **Enter**.

Chapter 3

Upgrading Connect:Enterprise UNIX

This document covers the information you need when upgrading to Connect:Enterprise UNIX Version 2.4.00 from a previous version of Connect:Mailbox UNIX or Connect:Enterprise UNIX.

The version of Connect:Enterprise 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
Connect:Enterprise 2.3	◆ *Upgrade Considerations for Version 2.4* on page 48 ◆ *Running the Installation Script for Releases 2.0 and Later* on page 51
Connect:Enterprise 2.2	◆ *Upgrade Considerations for Version 2.3* on page 48 ◆ *Upgrade Considerations for Version 2.4* on page 48 ◆ *Running the Installation Script for Releases 2.0 and Later* on page 51
Connect:Enterprise 2.1	◆ *Upgrade Considerations for Version 2.2* on page 49 ◆ *Upgrade Considerations for Version 2.3* on page 48 ◆ *Running the Installation Script for Releases 2.0 and Later* on page 51
Connect:Enterprise 2.0	◆ *Upgrade Considerations for Version 2.2* on page 49 ◆ *Upgrade Considerations for Version 2.3* on page 48 ◆ *Running the Installation Script for Releases 2.0 and Later* on page 51
Connect:Mailbox 1.3	◆ *Upgrade Considerations for a Release Prior to 2.0.00* on page 67 ◆ *Upgrade Considerations for Version 2.2* on page 49 ◆ *Upgrade Considerations for Version 2.3* on page 48 ◆ *Running the Installation Script for a Release Prior to 2.0* on page 69

Upgrade Considerations for Version 2.4

Consider the following information when upgrading from Connect:Enterprise version 2.3:

Encryption of Inbound AS2 Batches

If you had batch encryption enabled on the receiving mailbox on Connect:Enterprise version 2.3, inbound batches may not be encrypted in Connect:Enterprise version 2.4. 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 Connect:Enterprise version 2.4 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 Connect:Enterprise UNIX version 2.4, .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 Connect:Enterprise UNIX version 2.3 that is based on batch name, you will have to adjust your automation setup based on this new naming convention in Connect:Enterprise UNIX version 2.4.

Upgrade Considerations for Version 2.3

Consider the following information when upgrading from Connect:Enterprise version 2.2:

API Calls

The following API calls were added or updated in version 2.3. For additional information, refer to the *Connect:Enterprise UNIX Programmer's Guide*.

API Call	Update
APICMD_IDMBPASS_REFRESH	New for version 2.3
APICMD_CEUTRACE	New for version 2.3

Sample Programs

All sample programs must be recompiled.

Auto Connects (Schedules)

During the upgrade, the active auto connect queue, **ceuacq**, is replaced. You must restart any auto connects that are waiting in the queue.

Triple DES Batch Encryption

Triple DES Batch Encryption is not available immediately when upgrading. Refer to *Generating the Global Key (ceukey)* on page 155 to enable Triple DES batch encryption.

Security Exit for SSH

The Security Exit for SSH remote connections has changed from 3 to 10.

Upgrade Considerations for Version 2.2

Consider the following information when upgrading from Connect:Enterprise version 2.0.00, 2.1.00, or 2.1.01:

- The **ceustartup** and **ceustartup.trace** files are updated during installation with any new parameters. You no longer need to manually update your existing **ceustartup** and **ceustartup.trace** files.
- If you are upgrading from 2.1.00 or 2.1.01 with AS2 and you plan to encrypt the internal product communications (a new feature), perform the following procedure in addition to the procedures described in the *Encrypting Internal Product Communications* chapter of the *Connect:Enterprise UNIX Installation and Administration Guide*:
  a. Open the **cmuediint** and **cmuhttpd** scripts in the $CMUHOME/javalib directory.
  b. Set the **ceu.sipskey** system property to the location of the sipskey file. Following is an example:

```
propSettings="$propSettings -Dceu.sipskeys=$CMUHOME/keys/sipskeys"
```

API Calls

The following API calls were added or updated in version 2.2.

If you have existing API programs that issue an API command listed here, add any new arguments to your API program before recompiling for Connect:Enterprise UNIX version 2.4. If an argument was added that you do not use, pass the address of a null string. For additional information, refer to the *Connect:Enterprise UNIX Programmer's Guide*.

API Call	Update
APICMD_DAEMON_REFRESH	New for version 2.2
APICMD_SSLPASS_REFRESH	New for version 2.2
APICMD_SSHPASS_REFRESH	New for version 2.2
APICMD_CONNECT	The following argument was added: ◆ char *bpid
MBOXBATCH_INFO_T	The following argument was added for 64-byte support: ◆ ULONG ullBatchSize This affects APICMD_ADD, APICMD_DELETE, and APICMD_LIST.
APICMD_ERASE	The following arguments were added: ◆ char *szOrig ◆ char *szFlags ◆ ULONG ullBatchSize (added to MBOXBATCH_INFO_T)
APICMD_EXTRACT	The following arguments were added: ◆ char *szFrom ◆ char *szTo ◆ char *szOrig ◆ char *szFlags ◆ ULONG ullBatchSize (added to MBOXBATCH_INFO_T)
APICMD_ADD	The following argument was added: ◆ ULONG ullBatchSize (added to MBOXBATCH_INFO_T)
APICMD_DELETE	The following argument was added: ◆ ULONG ullBatchSize (added to MBOXBATCH_INFO_T)
APICMD_LIST	The following argument was added: ◆ ULONG ullBatchSize (added to MBOXBATCH_INFO_T)

User Exits

The makefile, cmuexits.c, and userlog.c user exits are named as follows:

- makefile.new_in_patch2200
- cmuexits.c.new_in_patch2200
- userlog.c.new_in_patch2200

In order to continue using the makefile, cmuexits.c, and userlog.c, you must merge any changes you have made in your existing exits, compile, and rename them makefile, cmuexits.c, and userlog.c.

All other existing user exits must be recompiled before they can be used. This includes the Batch Send, Batch Send 64, Batch Receive, and Batch Receive 64 exits. Refer to the *User Exits* chapter of the *Connect:Enterprise Programmer's Guide* for instructions.

The following user exits were added for version 2.0:

- CMUEXIT_BatchReceive64
- CMUEXIT_BatchSend64

Running the Installation Script for Releases 2.0 and Later

Use the following procedure to upgrade from Connect:Enterprise UNIX version 2.0 or later. This procedure describes how to access the Connect:Enterprise UNIX installation script, select the installation option, and specify the destination directory. You cannot install Connect:Enterprise 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 Connect:Enterprise installation from an ESD portal, navigate to the location of the **ceinstall** script.
   - If you acquired your Connect:Enterprise installation on a CD-ROM, mount the Connect:Enterprise UNIX CD-ROM.
2. At the UNIX prompt, type:

```
ceinstall
```

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

```
================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
Installation Procedure

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

Sterling Commerce, Inc.(TM) and Connect:Enterprise(TM) UNIX(TM) are trademarks
of Sterling Commerce, Inc. in the U.S.A. and other countries.

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/).
Media location:
```

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

Enter your choice:[2]
```

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

```
Connect:Enterprise UNIX base version n.n.nn will be installed on 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 Connect:Enterprise UNIX Version 2.4.00.
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 Connect:Enterprise UNIX 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
version Version 2.4.00 Upgrade Installation Procedure

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

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

Sterling Commerce, Inc.(TM) and Connect:Enterprise(TM) are
trademarks of Sterling Commerce, Inc. in the U.S.A. and other countries.

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_patch2400.

New files added by this update that you may wish to
merge with your current installation will be added as
<filename>.new_in_patch2400. A summary of these
will be written to /install_directory/merge.2400.

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

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

```
Installing from /xxxxxx/ceunix/Version 2.4.00/cebase2400s.cpio.


Installing Connect:Enterprise UNIX Version 2.4.00 ...

Approximately 310000 kbytes of disk space is required
to upgrade to Connect:Enterprise UNIX.
(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          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360  100357   40318   71% /
/dev/vg00/lvol1     295024   35632  229888   13% /stand
/dev/vg00/lvol8    1126400  729546  372184   66% /var
/dev/vg00/lvol7    1536000 1058958  447371   70% /usr
/dev/vg00/lvol4     716800   10648  662215    2% /tmp
/dev/vg00/lvol10   2048000 1764817  265865   87% /xxx
/dev/vg00/lvol9    1536000  442042 1025591   30% /qa
/dev/vg00/lvol6    1536000  825558  666092   55% /opt
/dev/vg00/lvol5     524288    1238  490364    0% /home
/dev/vg00/lvol11   5632000 3640645 1868525   66% /export1
/dev/datavg/data   34930688 12686712 22070392   37% /data
ahmi.csg.stercomm.com:/svshare
                   2492760 2217544  148584   94% /svshare
server:/space2    8705496 5700736 2917704   66% /space2

You have 265865 kbytes of disk space available to you,
which is more than the required 106000 kbytes.

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

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

```
You have chosen to install into "/install_directory".
Is this correct? [Y|n]
```

14. Type **Y** and press **Enter**. The following prompt is displayed:

```
 Connect:Enterprise UNIX files have been successfully upgraded and verified.
 Press Enter to continue the upgrade process.
```

15. The following is displayed:

```
web admin directory is being renamed to:
/data/ceunix/webservices/webapps/ceuadmin.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 additional 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.

Hit enter to continue.
```

Press **Enter** to continue.

16. 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/ceunix/mcd/control.mcd.new.parameters....
Review this file for the new MCD parameters.

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

17. 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 Connect:Enterprise.

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

```
Giving administrative privileges to RSD
```

Customizing Connect:Enterprise 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 functionality that you are currently using, the installation script detects your existing configuration. For example, if you are using a 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.

Setting Up Secure FTP

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

```
This product requires the use of an X.509 certificate.
You can generate a Certificate Signing Request (CSR) and verify
Key/Cert 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:

```
** Connect:Enterprise Secure FTP with SSL Setup Script **
Enter the path for your new private key: ["/usr/mailbox/ceunix/spd/privkey.txt"]
```

2. Type the complete path where you want to place your new private key, and press **Enter**. The following prompt is displayed:

```
Enter the path for your new Certificate Signing Request, a.k.a., CSR:
["/usr/mailbox/ceunix/spd/csr.txt"]
```

3. Type the complete path where you want to place your new Certificate Signing Request (CSR) and press **Enter**. The following prompt is displayed:

```
Would you like to encrypt your private key with a password? [y|N]:
```

Note: The default for this prompt is **No**.

4. Type **y** for the additional security of encrypting your private key with a password. Type **n** (or press **Enter**) if you do not want to use a password.

Note: If you type **y**, you are prompted to enter and verify a password. Your private key password can be up to 256 characters.

The following prompt is displayed:

```
Enter length (in bits) of your private key (512-2048): [1024]
```

5. Type the length of your private key in bits and press **Enter**. It can be any length between 512 and 2048 bits. The default is 1024.

   The utility to generate an SSL Certificate Signing Request starts, using the files specified in the previous steps. A screen, similar to the following, is displayed:

```
**** running 'cmusslgencsr -k /usr/mailbox/ceunix/spd/privkey.txt
-c /usr/mailbox/ceunix/spd/csr.txt -l 1024 '
**
# Connect:Enterprise UNIX Private Key and CSR Generation Utility #
# Setting Up #
# Generating RSA key pair [1024-bit]
#Using default password 'password'
# File '/usr/mailbox/ceunix/spd/privkey.txt' contains your encrypted private
key #
#Generating Certificate Signing Request #
2 Letter Country Code (max 2 characters):
```

6. Type your two-letter country code and press **Enter**. The following prompt is displayed:

```
State/Province (max 128 characters):
```

7. Type the name of your state or province and press **Enter**. The following prompt is displayed:

```
City/Locality (max 128 characters):
```

8. Type the name of your city or locality and press **Enter**. The following prompt is displayed:

```
Organization Name (max 128 characters):
```

9. Type the name of your organization and press **Enter**. The following prompt is displayed:

```
Organizational Unit (max 128 characters):
```

10. Type the name of your organizational unit and press **Enter**. The following prompt is displayed:

```
Common Name (server host name) (max 128 characters):
```

11. Type the host name of your server and press **Enter**.

    A screen, similar to the following, is displayed:

```
# You may submit file 'usr/mailbox/ceunix/spd/csr.txt' to your CA to request a
certificate #

Private key and CSR generated successfully.  You may now submit your CSR to a CA,
from which you should then receive a certificate.  You should then concatenate the
certificate with your private key to create your Key/Cert file.
```

Note: For instructions on requesting, distributing, and installing certificates, refer to Chapter 9, *Secure FTP*.

    The following prompt is displayed:

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

12. Type the number corresponding to the level of security you want to implement and press **Enter**. 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]
```

13. Type the number corresponding to the appropriate cipher strength for the sites with which you exchange data and press **Enter**. See Chapter 9, *Secure FTP* in the *Connect:Enterprise UNIX Installation and Administration Guide* for more information regarding cipher suites.

    The next screen allows you to complete the Secure FTP installation.

```
Enter the FULL path where you will place your Key/Cert file:
["usr/mailbox/ceunix/spd/keycert.txt"]
```

14. Type the path to the directory where you would like to create a placeholder for the Key/Cert file and press **Enter**. See Chapter 9, *Secure FTP* in the *Connect:Enterprise UNIX Installation and Administration Guide* for a description of the Key/Cert file.

    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 9, *Secure FTP* in the *Connect:Enterprise UNIX Installation and Administration Guide* for more information.

Setting Up SSH

You are prompted to configure 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* **cmusshcust** script.

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

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

2. Type the TCP/IP port number that the 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 hit 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. 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/users/user01/ceunix2200s/ssh/system/host_key
Your public key is being saved in:
 /data/users/user01/ceunix2200s/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.

If a passphrase was used for building the ssh_host_key, you will have
to run 'cmurefresh -s <passphase>' after bringing up the SSH Server.
------------------------------------------------------------------------

Would you like to build a keypair for the samp_ssh example? [Y|n
```

8. You can specify to create a key pair 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 62. 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/users/user01/ceunix2200s/ssh/users/samp_ssh/id_rsa
   Your public key is being saved in:
    /data/users/user01/ceunix2200s/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 13, *Configuring High Availability*, in the *Connect:Enterprise UNIX Installation and Administration Guide* 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/ceunix21
was detected to be the location of Connect:Enterprise Secure FTP.

Is this correct? [Y|n]
```

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

```
================================================================================
Sterling Commerce, Inc., (TM) Connect:Enterprise UNIX (TM)
Version n.n High-Availability Package Installation Procedure

The Connect:Enterprise 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 Connect:Enterprise 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) Unix(TM)
version n.n.nn  Customization

This customization procedure sets up AS2 for Connect:Enterprise 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**. The following prompt is displayed:

```
Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version x.x.xx     at /usr/java/jdkx.x.xx/bin/java
2 = version x.x.xx     at /usr/java/jdkx.x.xx/jre/bin/java
Select [0-2]:
```

3. Select the Java version to use and press **Enter**. The installation proceeds and the script returns to the customization script.

Setting Up the HTTP Server

Connect:Enterprise 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 tp 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:

```
Enter port number for the HTTP Services daemon listener [8002]
```

2. 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**.

   If you did not select to configure AS2, the following prompt is displayed:

```
Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version x.x.xx     at /usr/java/jdkx.x.xx/bin/java
2 = version x.x.xx     at /usr/java/jdkx.x.xx/jre/bin/java
Select [0-2]:
```

3. Select the Java version to use and press **Enter**. The following prompt is displayed:

```
Created script: /sci/users/user01/ceunix2200s/javalib/cmuadmind
Updating ceuadmin's system.properties file with:
   addr = hostname
   port = port#
Found jar at /usr/j2se/bin/jar
adding: property/(in = 0) (out= 0)(stored 0%)
adding: property/system.properties(in = 178) (out= 76)(deflated 57%)

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

For WebDAV access use:
http://hostname:port#/ceuadmin/jsp/index.jsp
Hit enter to continue.
```

4. The installation proceeds and the script returns to the installation menu.

Completing the Installation

After all components are installed, the customization script continues with the following prompt:

```
....Creating ceustartup script....

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

....Creating ceushutdown script....
```

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

```
================================================================================
To Start Connect:Enterprise UNIX, you must install the license management key
included with your shipment. The key shipped
with the product is a temporary key and must be replaced with a permanent
key that you request from your Sterling Commerce account representative.
The license management key must be installed and renamed to
/$CMUHOME/etc/license.key.
Please refer to the Installation and Administration Guide for instructions.
================================================================================

Please press ENTER to continue...
```

2. Press **Enter** to continue the installation. The following prompt is displayed:

```
Connect:Enterprise UNIX configuration completed.

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

export CMUHOME=/$CMUHOME/ceunix2
export CMUHOST=cmuhostname
export CMUPORT=xxxx
export PATH=$PATH:$CMUHOME/etc:$CMUHOME/os/bin
export LD_LIBRARY_PATH=${CMUHOME}/os/lib
export LIBPATH=${CMUHOME}/os/lib
export SHLIB_PATH=${CMUHOME}/os/lib


You can set the environment variables later by executing
/$CMUHOME/etc/profile
at shell prompt

OR

incorporate $CMUHOME/etc/profile into
your environment.


================================================================================

Please press ENTER to continue...
```

3. Press **Enter** to continue the installation. The following prompt is displayed:

```
================================================================
Connect:Enterprise UNIX configuration completed.

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

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

Connect:Enterprise UNIX base version 2.4.00 install successful.

Would you like to return to the Connect:Enterprise UNIX
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.

4. To return to the Connect:Enterprise UNIX installation menu, press **Enter**. If you completed the installation, type **n** and press **Enter**. A command prompt is displayed.
5. After the upgrade completes successfully, refer to the Chapter 4, *Post-Installation Tasks*.

Upgrade Considerations for a Release Prior to 2.0.00

Review the information in this section before you begin upgrading.

Validating and Backing Up Your Repository Contents

Your repository will be converted. However, if your repository is corrupt, the conversion may fail. To ensure that the contents of your repository are not corrupt, run the **cmufixup** utility before you begin the upgrade. The **cmufixup** utility validates that the *$CMUHOME/med* file exists and that the entries in the control file match the actual data batches in the repository. See the *Administrator Commands* chapter of the *Connect:Enterprise Installation and Administration Guide* for details on how the **cmufixup** utility works and instructions on how to use it.

After you verify your repository contents, be sure to back up your repository database before you run the upgrade installation script.

During the installation, the upgrade program detects whether your repository is c-tree 7.12. For best results, if you are prompted to convert your repository, select **Yes**. However, if you select **No**, you can convert your repository to the database format using the **ceucvtrep** utility with the following parameters.

Caution: Back up your repository before running this utility.

Parameter	Description
-c *cmuhome_directory_path*	Specifies the location of the $CMUHOME/database directory. If you do not specify this parameter, the value will be taken from the $CMUHOME environment variable, if it exists.
-?|h --help	Displays usage information.

Following is an example:

```
ceucvtrep -c server1/ceunix/database
```

Log File Format Upgrade

The log file format has changed. The log files you are currently writing to are converted automatically to the new format and are available using the **cmureport** command or the Connect:Enterprise Site Administration user interface.

Your archived log files are saved into the $CMUHOME/oldlog.*mm.dd.yyyy* directory with the directory name oldlog.*mm.dd.yyyy*, where *mm.dd.yyyy* is the date that you run the upgrade script.

Note: If you have a logacct.dat file that ends with the .new extension, such as logacct.new, the log file will not be converted during the upgrade. Use the **ceucvtlog** command described below to convert the file after installation.

These archived log files are not available using the **cmureport** command or the Site Administration user interface. They are only available using the **cmureport.*platform*.old** utility, which is also saved in the $CMUHOME/oldlog.*mm.dd.yyyy* directory. The **cmureport.*platform*.old** utility allows you to perform all functions of cmureport on previously archived log files (*platform* is the UNIX platform you are running on).

You can convert archive log files that are in the $CMUHOME/oldlog.*mm.dd.yyyy* to the new format using **ceucvtlog** utility with the following parameters:

Parameter	Description
-i *input_log_file*	Specifies the name of the log file you want to convert. This parameter is required.
-o *new_log_file* --output *new_log_file*	Specifies the name of the log file after it is converted. This parameter is required.
-f *format* --format *[v1|v2]*	Specifies to convert a log file to the new log format (v1) or to the old log format (v2). This parameter is required.
-?|h --help	Displays usage information.

Following is an example:

```
ceucvtlog -i log_archive1 -o log_archive_convert1 -f v1
```

This command converts the log file so it is available using the **cmureport** utility and not the **cmureport.*platform*.old** utility.

You can also use the **ceucvtlog** utility to convert log files back to the old format.

Startup Scripts

New startup scripts **ceustartup** and **ceustartup.trace** are added. The old scripts will be saved in the $CMUHOME/etc directory with the names **ceustartup.*mm.dd.yyyy*** and **ceustartup.trace.*mm.dd.yyyy,*** where *mm.dd.yyyy* is the date that you run the upgrade script. You need to merge any changes you have made into the new **ceustartup** and **ceustartup.trace** scripts, also located in the $CMUHOME/etc directory.

Add Path to the javalib Directory

You will need to add the path to the $CMUHOME/javalib directory to the following files:

- $CMUHOME/cshrc
- $CMUHOME/kshrc

Following is an example:

```
set path=($path  $CMUHOME/etc $CMUHOME/hpux/bin $CMUHOME/javalib)
PATH=$PATH:$CMUHOME/etc:$CMUHOME/hpux/bin:$CMUHOME/java
```

High Availability

If you are using a high-availability system, you will need to modify the proc_mon.cfg file by adding the following daemons:

- Service Interface daemon (cmusvid). Following is an example:

```
cmusvid:process_owner:core:cmusvid -H hostname -P portno -p portno -l debug -d
debugfile
```

  Refer to the *cmusvid—Service Interface Daemon* section and the *Connect:Enterprise High Availability* chapter of the *Connect:Enterprise Installation and Administration Guide.*

- Authentication Server daemon (cmauthd). Following is an example:

```
cmuauthd:process_owner:core:cmusvid -H hostname -P portno -p portno -l debug -d
debugfile
```

  Refer to the *cmuauthd—Authentication Server Daemon* section and the *Connect:Enterprise High Availability* chapter of the *Connect:Enterprise Installation and Administration Guide.*

Running the Installation Script for a Release Prior to 2.0

Use the following procedure to upgrade from a release prior to Connect:Enterprise UNIX Version 2.0. This procedure describes how to access the Connect:Enterprise UNIX installation script, select the installation option, and specify the destination directory. You cannot install Connect:Enterprise 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 Connect:Enterprise installation from an ESD portal, navigate to the location of the **ceinstall** script.
   - If you acquired your Connect:Enterprise installation on a CD-ROM, mount the Connect:Enterprise UNIX CD-ROM.

2. At the UNIX prompt, type:

```
ceinstall
```

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

```
============================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
Installation Procedure

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

Sterling Commerce, Inc.(TM) and Connect:Enterprise(TM) UNIX(TM) are trademarks
of Sterling Commerce, Inc. in the U.S.A. and other countries.

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/).
Media location:
```

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

Enter your choice:[2]
```

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

```
Connect:Enterprise UNIX base version n.n.nn will be installed on 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 Connect:Enterprise UNIX Version 2.4.00.
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 Connect:Enterprise UNIX 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
version Version 2.4.00 Upgrade Installation Procedure

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

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

Sterling Commerce, Inc.(TM) and Connect:Enterprise(TM) are
trademarks of Sterling Commerce, Inc. in the U.S.A. and other countries.

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

Press ENTER when ready.
```

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_patch2400.

New files added by this update that you may wish to
merge with your current installation will be added as
<filename>.new_in_patch2400. A summary of these
will be written to /install_directory/merge.2400.

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

12. A prompt similar to the following is displayed:

```
================================================================================

This release includes significant internal changes to support
increased batch sizes. If you are upgrading from a version previous
to 2.0.00, the internal repository format, the log file format,
the exits interfaces, and the command API interface are changed. Any
user API programs and programs that process log file records will need
to be recreated to work with the new release. Please carefully
review the product Release Notes before performing the new
installation.


Execution of this upgrade script will cause existing Connect:Enterprise
UNIX binaries to be replaced with release n.n versions. Once this is
completed, the converted database, log files, and new binaries will
not be compatible with prior releases of Connect:Enterprise UNIX. For
this reason, we strongly recommend you back up your entire installation
before proceeding!

================================================================================

Do you wish to proceed with the installation? [Y/n]
```

13. Press **Enter**. The installation proceeds until you are prompted with something similar to the following:

```
================================================================================
The repository will be converted by this upgrade script.
If it is corrupted, the conversion may fail.

If the conversion does fail, you will have to restore your existing system.

To ensure that the repository contents are not corrupted, it is highly
suggested that you run cmufixup before doing this upgrade.
================================================================================

Do you wish to continue with the upgrade? [Y/n]
```

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

```
Log information has been preserved in
/xxx/xxxxx/xxxxxx/ceunix13/oldlog.05.22.2003,
including a copy of cereport and cmureport.


Installing from /xxxxxx/ceunix/n.n.nn/cebase2400s.cpio.


Installing Connect:Enterprise UNIX n.n.nn ...

Approximately 106000 kbytes of disk space is required
to upgrade to Connect:Enterprise UNIX.
(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          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360  100357   40318   71% /
/dev/vg00/lvol1     295024   35632  229888   13% /stand
/dev/vg00/lvol8    1126400  729546  372184   66% /var
/dev/vg00/lvol7    1536000 1058958  447371   70% /usr
/dev/vg00/lvol4     716800   10648  662215    2% /tmp
/dev/vg00/lvol10   2048000 1764817  265865   87% /xxx
/dev/vg00/lvol9    1536000  442042 1025591   30% /qa
/dev/vg00/lvol6    1536000  825558  666092   55% /opt
/dev/vg00/lvol5     524288    1238  490364    0% /home
/dev/vg00/lvol11   5632000 3640645 1868525   66% /export1
/dev/datavg/data   34930688 12686712 22070392   37% /data
ahmi.csg.stercomm.com:/svshare
                   2492760 2217544  148584   94% /svshare
server:/space2    8705496 5700736 2917704   66% /space2

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

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

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

```
You have chosen to install into "/install_directory".
Is this correct? [Y/n]
```

16. Type **Y** and press **Enter**. The following prompt is displayed:

```
Connect:Enterprise UNIX files have been successfully upgraded and verified.
Press Enter to continue the upgrade process.
```

17. Press **Enter**. The installation files are extracted. A prompt similar to the following is displayed:

```
The existing log files and report programs have been saved in the
/xxx/xxxxx/xxxxxx/ceunix13/oldlog directory. These are incompatible with
the new release of Connect:Enterprise UNIX. Please note also that the
log file conversion utility ceucvtlog is provided with this release.

The existing repository structure is incompatible with the new release.
The repository must be converted to the new format before starting
Connect:Enterprise UNIX.

Do you wish to convert the repository and log files now? [Y/n]
```

18. If you have not backed up your repository, do that before continuing. If you have backed up your repository, press **Enter** to continue. A prompt similar to the following is displayed:

```
Checking current repository format.
The repository in /xxx/xxxxx/xxxxxx/ceunix13/database/mailbox seems to be empty.

Checking access to control files and utilities.

Ready to convert the repository.

Control directory in /xxx/xxxxx/xxxxxx/ceunix13/database
Data directory in /xxx/xxxxx/xxxxxx/ceunix13/database/mailbox
MED file in /xxx/xxxxx/xxxxxx/ceunix13/med/cmumbox.med

It is recommended to backup the repository prior to performing the conversion.
Do you wish to continue? [Y/n]
```

19. 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 Connect:Enterprise.

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

```
Please enter the Connect:Enterprise UNIX RSD password [userID]:
```

20. Type type password associated with userID and press **Enter**.

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 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 customize Connect:Enterprise UNIX.

Setting Up Secure FTP

If you have Connect:Enterprise Secure FTP, the customization script continues with the following prompt:

```
This product requires the use of an X.509 certificate.
You can generate a Certificate Signing Request (CSR) and verify
Key/Cert 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:

```
** Connect:Enterprise Secure FTP with SSL Setup Script **
Enter the path for your new private key: ["/usr/mailbox/ceunix/spd/privkey.txt"]
```

2. Type the complete path where you want to place your new private key, and press **Enter**. The following prompt is displayed:

```
Enter the path for your new Certificate Signing Request, a.k.a., CSR:
["/usr/mailbox/ceunix/spd/csr.txt"]
```

3. Type the complete path where you want to place your new Certificate Signing Request (CSR) and press **Enter**. The following prompt is displayed:

```
Would you like to encrypt your private key with a password? [y|N]:
```

Note: The default for this prompt is **No**.

4. Type **y** for the additional security of encrypting your private key with a password. Type **n** (or press **Enter**) if you do not want to use a password.

Note: If you type **y**, you are prompted to enter and verify a password. Your private key password can be up to 256 characters.

The following prompt is displayed:

```
Enter length (in bits) of your private key (512-2048): [1024]
```

5. Type the length of your private key in bits and press **Enter**. It can be any length between 512 and 2048 bits. The default is 1024.

The utility to generate an SSL Certificate Signing Request starts, using the files specified in the previous steps. A screen, similar to the following, is displayed:

```
**** running 'cmusslgencsr -k /usr/mailbox/ceunix/spd/privkey.txt
-c /usr/mailbox/ceunix/spd/csr.txt -l 1024 '
**
# Connect:Enterprise UNIX Private Key and CSR Generation Utility #
# Setting Up #
# Generating RSA key pair [1024-bit]
#Using default password 'password'
# File '/usr/mailbox/ceunix/spd/privkey.txt' contains your encrypted private
key #
#Generating Certificate Signing Request #
2 Letter Country Code (max 2 characters):
```

6. Type your two-letter country code and press **Enter**. The following prompt is displayed:

```
State/Province (max 128 characters):
```

7. Type the name of your state or province and press **Enter**. The following prompt is displayed:

```
City/Locality (max 128 characters):
```

8. Type the name of your city or locality and press **Enter**. The following prompt is displayed:

```
Organization Name (max 128 characters):
```

9. Type the name of your organization and press **Enter**. The following prompt is displayed:

```
Organizational Unit (max 128 characters):
```

10. Type the name of your organizational unit and press **Enter**. The following prompt is displayed:

```
Common Name (server host name) (max 128 characters):
```

11. Type the host name of your server and press **Enter**.

    A screen, similar to the following, is displayed:

```
# You may submit file 'usr/mailbox/ceunix/spd/csr.txt' to your CA to request a
certificate #

Private key and CSR generated successfully.  You may now submit your CSR to a CA,
from which you should then receive a certificate.  You should then concatenate the
certificate with your private key to create your Key/Cert file.
```

Note: For instructions on requesting, distributing, and installing certificates, refer to Chapter 9, *Secure FTP* in the *Connect:Enterprise Installation and Administration Guide*.

The following prompt is displayed:

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

12. Type the number corresponding to the level of security you want to implement and press **Enter**. 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]
```

13. Type the number corresponding to the appropriate cipher strength for the sites with which you exchange data and press **Enter**. See Chapter 9, *Secure FTP* in the *Connect:Enterprise Installation and Administration Guide* for more information regarding cipher suites.

    The next screen allows you to complete the Secure FTP installation.

```
Enter the FULL path where you will place your Key/Cert file:
["usr/mailbox/ceunix/spd/keycert.txt"]
```

14. Type the path to the directory where you would like to create a placeholder for the Key/Cert file and press **Enter**. See Chapter 9, *Secure FTP* in the *Connect:Enterprise Installation and Administration Guide* for a description of the Key/Cert file.

    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 9, *Secure FTP* in the *Connect:Enterprise Installation and Administration Guide* for more information.

Setting Up SSH

The customization script prompts you to configure 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* **cmusshcust** script.

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

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

2. Type the TCP/IP port number that the 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 hit 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. 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/users/user01/ceunix2200s/ssh/system/host_key
Your public key is being saved in:
 /data/users/user01/ceunix2200s/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.

If a passphrase was used for building the ssh_host_key, you will have
to run 'cmurefresh -s <passphase>' after bringing up the SSH Server.
------------------------------------------------------------------------

Would you like to build a keypair for the samp_ssh example? [Y|n
```

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 62. 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/users/user01/ceunix2200s/ssh/users/samp_ssh/id_rsa
Your public key is being saved in:
 /data/users/user01/ceunix2200s/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

The customization script prompts you 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 13, *Configuring High Availability* in the *Connect:Enterprise Installation and Administration Guide* 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/ceunix21
was detected to be the location of Connect:Enterprise Secure FTP.

Is this correct? [Y|n]
```

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

```
================================================================================
Sterling Commerce, Inc., (TM) Connect:Enterprise UNIX (TM)
Version n.n High-Availability Package Installation Procedure

The Connect:Enterprise 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 Connect:Enterprise UNIX
High-Availability Package Installation Guide.
================================================================================
Press Enter...
```

Setting Up AS2

The customization script prompts you 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) Unix(TM)
version n.n.nn  Customization

This customization procedure sets up AS2 for Connect:Enterprise 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**. The following prompt is displayed:

```
Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version x.x.xx     at /usr/java/jdkx.x.xx/bin/java
2 = version x.x.xx     at /usr/java/jdkx.x.xx/jre/bin/java
Select [0-2]:
```

3. Select the Java version to use and press **Enter**. The installation proceeds and the script returns to the customization script.

Setting Up the HTTP Server

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

The customization script continues with the following prompt.

```
Do you want to configure 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:

```
Enter port number for the HTTP Services daemon listener [8002]
```

2. 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**.

   If you did not select to configure AS2, the following prompt is displayed:

```
Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version x.x.xx     at /usr/java/jdkx.x.xx/bin/java
2 = version x.x.xx     at /usr/java/jdkx.x.xx/jre/bin/java
Select [0-2]:
```

3. Select the Java version to use and press **Enter**. The following prompt is displayed:

```
Created script: /sci/users/user01/ceunix2200s/javalib/cmuadmind
Updating ceuadmin's system.properties file with:
   addr = hostname
   port = port#
Found jar at /usr/j2se/bin/jar
adding: property/(in = 0) (out= 0)(stored 0%)
adding: property/system.properties(in = 178) (out= 76)(deflated 57%)

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

Hit enter to continue.
```

4. The installation proceeds and the script returns to the installation script.

Completing the Installation

After all components are installed, including Connect:Direct UNIX, the customization script continues with the following prompt:

```
Initializing Databases and Creating Admin Role

Creating Mailbox Database
Date: 04/21/03Connect:Enterprise for UNIXPage: 1
Time: 16:44:21Initialize Mailbox

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

Creating / Updating Roles Database ...

Successfully created data files and indices

Roles database: Complete!!!

Creating Admin Role

The administrator roles and accounts were created successfully.

....Creating ceustartup script....

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

....Creating ceushutdown script....
Please press ENTER to continue...
```

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

```
================================================================================
To Start Connect:Enterprise UNIX, you must install the asset
protection Keyfile included with your shipment. The Keyfile shipped
with the product is a temporary key and must be replaced with a permanent
key that you request from your Sterling Commerce account representative.
The license file must be installed and renamed to
/$CMUHOME/etc/license.key.
Please refer to the Installation and Administration Guide for instructions.
================================================================================

Please press ENTER to continue...
```

Chapter 4

Post-Installation Tasks

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

- Exporting the environment variables
- Installing the license management key file
- 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 Connect:Enterprise.

Exporting the Environment Variables

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

```
Connect:Enterprise UNIX configuration completed.

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

export CMUHOME=/$CMUHOME/ceunix2
export CMUHOST=cmuhostname
export CMUPORT=xxxx
export PATH=$PATH:$CMUHOME/etc:$CMUHOME/os/bin
export LD_LIBRARY_PATH=${CMUHOME}/os/lib
export LIBPATH=${CMUHOME}/os/lib
export SHLIB_PATH=${CMUHOME}/os/lib

You should set environment variables later by either executing
. /$CMUHOME/etc/profile
at shell prompt

OR

incorporating $CMUHOME/etc/profile into
your environment.

================================================================================
Please press ENTER to continue...
```

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

Note: If you upgraded from a previous version of Connect:Enterprise UNIX or 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 Connect:Enterprise.

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

Installing the License Key File

The license key file identifies the product features that are available at a site. When you purchase the Connect:Enterprise UNIX application, a temporary key file is sent to you that enables operation of Connect:Enterprise UNIX for a limited time. You must replace the temporary key with a permanent key to continue running Connect:Enterprise UNIX.

During the Connect:Enterprise UNIX installation, you are given information on installing the license management key file. The license management key file is installed after the Connect:Enterprise installation script has been executed.

```
================================================================================
To Start Connect:Enterprise UNIX, you must install the license management key
included with your shipment. The key shipped
with the product is a temporary key and must be replaced with a permanent
key that you request from your Sterling Commerce account representative.
The license management key must be installed and renamed to
/$CMUHOME/etc/license.key.
Please refer to the Installation and Administration Guide for instructions.
================================================================================

Please press ENTER to continue...
```

The temporary and permanent key files are supplied as text files named *nnnnn*.txt, where *nnnnn* is a number assigned by Sterling Commerce. Each key file is sent to you as an attachment to an e-mail. The temporary and permanent license key file must be applied on the computer where Connect:Enterprise UNIX is installed.

To apply the temporary and permanent key file:

1. Copy the temporary license key file from the Sterling Commerce e-mail to the **$CMUHOME/etc** directory.
2. Rename the temporary license key file to **license.key**.

Caution: Do not edit the *nnnnn*.txt file or the license.key file. Text editors may insert a carriage return or truncate lines, which will invalidate the key file.

3. Request the permanent license key file using one of the following methods:
   - Reply to the Sterling Commerce e-mail containing your temporary license key file and include the host name of the computer where Connect:Enterprise UNIX is installed.
   - Request the license key file from Support On Demand:
     - Log in to the Sterling Commerce Support On Demand Web site. If you do not have a Support On Demand user name and password, follow the instructions in the *Getting Support for Sterling Commerce Products* section of the *Connect:Enterprise UNIX Version 2.4.00 Release Notes*.
     - Under Product Family Support, highlight **Connect** and click **Key Request**. The Connect Product Key Request page is displayed.
     - Type the information in the required fields and click **Submit**.
     - You will receive the permanent license key file through e-mail in approximately 24 to 48 hours.
4. Make a copy of the original permanent license key file and keep it in a safe place.
5. Repeat steps 1 and 2 to replace the temporary license key file with the permanent key file.

Testing the Installation

Prior to starting Connect:Enterprise, the installation may be tested using **cmu_quick_test**. After running **cmu_quick_test**, continue with the *Setting Up the Connect:Enterprise UNIX Site Administration User Interface* on page 94.

The following steps give instructions on running the test script:

1. Type the following command:

```
cmu_quick_test
```

   The test script starts.

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) UNIX(TM)
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 Connect:Enterprise UNIX home directory:
[/usr/mailbox/ceunix]:
```

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

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

Starting Connect:Enterprise(TM) system...
```

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

```
Connect:Enterprise UNIX V2.4.00
Mailbox Control Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820


Connect:Enterprise UNIX V2.4.00
Authentication Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820


Connect:Enterprise UNIX Vn.n.nn
Mailbox Engine Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX Vn.n.nn
Auto connect Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX Vn.n.nn
Log Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX V2.4.00
Exits Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX V2.4.00
Service Interface Daemon
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820
```

```
Connect:Enterprise UNIX V2.4.00
FTP Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX V2.4.00
SSH FTP Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Please press ENTER to run cmusession...
```

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

```
Date: 08/30/01          Connect:Enterprise UNIX  2.4.00        Page: 0001
Time: 17:01:24                   Session Utility

Command Line Parameters:
     cmusession


Name        Type    Host      PID     RmtID Resource   State         SID


FTP        Master   honolulu  10359    0     10029       Idle          5
ACD        Master   honolulu  10353    0                 -             3


Max. Concurrent Sessions: 0


Please press ENTER to run cmuadd...
```

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

```
Date: 08/30/01          Connect:Enterprise UNIX   2.4.00         Page: 0001
Time: 17:01:26                  ADD Utility

Command Line Parameters:
     cmuadd
     -iuser1
     -btest batch
     -m

Mbx ID    Batch #   Batch ID        Bytes      Date-Time     Status    Org ID


user1    15       test batch       100     01/08/30-17:01  ARMZ       user1

Input Files Processed
File Name       File Size       Pr Status

Summary Information
Number of Batches Added:     1

Date: 08/30/00           Connect:Enterprise UNIX 2.4.00        Page: 0002
Time: 17:01:26                  ADD Utility


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



Please press ENTER to run cmulist...
```

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: 08/30/01           Connect:Enterprise UNIX  2.4.00          Page: 0001
Time: 17:01:27                  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 ID        Bytes      Date-Time     Status    Org ID

Date: 08/30/01           Connect:Enterprise UNIX              Page: 0002
Time: 17:01:27                  LIST Utility

user1    15       test batch       100     01/08/30-17:01  ARMZ       user1


Please press ENTER to continue ....
sun ceushutdown ...
```

8. Press **Enter** to continue.

```
 End of 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 Connect:Enterprise UNIX Site Administration User Interface

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 ceuadmin.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/ceuadmin/property
   ```

   where *Deploy_Directory* is the directory where the ceuadmin.war file is deployed.

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

3. Verify that the system.properties file identifies the correct host name and port where the Connect:Enterprise UNIX service daemon is running. This information was required in *step 8 on page 21 of Before You Begin* on page 19. The default the installation script provides is 8001.
4. Start or restart your Web server.
5. Use the following URL to run the Connect:Enterprise UNIX Site Administration User Interface:

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

6. Log on to the Connect:Enterprise 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 Connect:Enterprise 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 Connect:Enterprise 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 110 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/ceuadmin/WEB-INF
  ```

  where *Deploy_Directory* is the directory where the ceuadmin.war file is deployed.

  Note: This directory may also be *Deploy_Directory*/ceuadmin.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 Connect:Enterprise 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.

Chapter 5

Starting and Stopping Connect:Enterprise

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

Startup Script

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 Connect:Enterprise for the first time. For information on how to modify the **ceustartup** script, see the *Modifying Startup Scripts* on page 99.

Starting Connect:Enterprise with ceustartup

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

```
ceustartup
```

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.

```
Connect:Enterprise UNIX V2.4.00
Mailbox Control Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820


Connect:Enterprise UNIX V2.4.00
Authentication Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820


Connect:Enterprise UNIX Vn.n.nn
Mailbox Engine Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX Vn.n.nn
Auto connect Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX Vn.n.nn
Log Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX V2.4.00
Exits Server
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820

Connect:Enterprise UNIX V2.4.00
Service Interface Daemon
Copyright  1994,1999,2006 Sterling Commerce, Inc.
Connect:Enterprise is a trademark of Sterling Commerce, Inc.
All rights reserved.
U.S. Patent Number 5,734,820
```

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 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 Connect:Enterprise.

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

You can also trace Connect:Enterprise resources using the dynamic tracing feature. Refer to *Tracing Connect:Enterprise Activity* on page 166.

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 99.

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

1. Before starting 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 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***, **cmusshhftpd**.

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 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 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 Connect:Enterprise can be served by a single FTP daemon with no Async or Bisync daemons. Another 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 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 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.

Parameter	Description
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 *$CMUHOME/mcd/control.mcd.*
-d	debugfile	Specifies the debug message output file name.
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.

Parameter	Value	Description
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-r	directory of RSD files	Specifies another directory location for the RSD files, rather than the default of *$CMUHOME/rsd*. ***Caution*:** 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 Connect:Enterprise 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	*seconds*	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.

Command	Parameter	Associated Values
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ 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.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce 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*, *cmuftpd*, *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 *$CMUHOME/mcd/control.mcd.*
-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.
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.

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. Valid values range from 1 to 1024 inclusive. The default value of 50 is sufficient for all but the most active systems. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-r	<none>	Specifies that the ***mbxacl.conf*** file is used to enact restricted access for mailbox security. If **-r** is not specified, all users have full access to all mailboxes.
-s	system administrator	Only valid if **-r** is used. The **-s** allows the account that started the Mailbox daemon to designate another account as the system administrator. If **-s** is not specified with **-r** in effect, the system administrator is the account that started the Mailbox daemon.
-?|-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, Connect:Enterprise UNIX is shutdown.
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-S	pipe name	Specifies the name and location of the cmuuserlog utility: $CMUHOME/arch.bin/cmuuserlog

Parameter	Values	Description
-?|-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 requeuing 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 queueing 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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-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.

Parameter	Values	Description
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-r	ACD directory	Overrides the default ACD directory path name. The default is *$CMUHOME/acd*. ***Caution*:** 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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-I	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.
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-?|-h		Displays the usage message.

cmusvid—Service Interface Daemon

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

Command	Parameter	Associated Values
-d	debugfile	Specifies the debug message output file name.
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-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.
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ 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.
-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 50 is sufficient for all but the most active systems. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-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 Connect:Enterprise UNIX to provide an internal Java HTTP server and servlet for the Connect:Enterprise 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 Connect:Enteprise 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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ Value passed on the command line using the **-H** parameter ◆ Value of the CMUHOST environment variable ◆ Value of the gethostname() system call ◆ Literal value of *localhost*

Command	Parameter	Associated Values
-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.
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ 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.
-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 fails.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-x	max sessions	Specifies the maximum number of sessions with the Site Administration user interface that are supported. The default value is 20.
-T	timeout	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.
-?|-h		Displays the usage message.

cmuasyd—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 *$CMUHOME/cpd/async.cpd*.
-d	debugfile	Specifies the debug message output file name.
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.
-N	*daemon Name*	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 **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.

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. Valid values range from 1 to 1024 inclusive. The default value of 20 is sufficient for all but the most active systems. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-?|-h		Displays the usage message.

cmuftpd—FTP Daemon

There are four distinct FTP daemons: ***cmuftpd*** (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 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 Connect:Enterprise FTP client to traverse intermediate FTP proxy servers. Secure FTP cannot be used with FTP proxy firewalls.

The FTP daemon in 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, ***cmuftpd*** does not use this binary. To use the binary to cross the SOCKS firewall, start ***cmuftpd*** 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 ***cmuftpd*** is executing, an FTP login can be made with Connect:Enterprise to begin a remote connect session. When remote connects occur, log messages are sent by ***cmuftpd*** 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.

cmuftpd Parameters

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

Parameter	Value	Description
-C	CPD configuration file	Overrides the default CPD file name. The default is *$CMUHOME/cpd/ftp.cpd*.
-c	FTP client pathname	Overrides the **FTP client path** 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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ Value passed on the command line using the **-H** parameter ◆ Value of the CMUHOST environment variable ◆ Value of the gethostname() system call ◆ Literal value of *localhost*
-l	debug level	Specifies the debug message level.

Parameter	Value	Description
-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: ◆ batch is requestable ◆ batch has not been transmitted and is not in the process of being transmitted ◆ batch is not marked incomplete ◆ batch has not been deleted
-K	*n*	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. Valid values: 0 - no keep alive is set 1 - keep alive for autoconnect only 2 - keep alive for remote connect only 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 **Listener Port** 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 *oldfilename newfilename* command. For information on the RENAME command, refer to the *Standard FTP Commands* chapter of the *Connect:Enterprise UNIX Remote User's Guide*.
-N	*daemon Name*	Overrides the default daemon name of FTP. Daemon names should be 8 characters or less with no spaces.

Parameter	Value	Description
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-s	ftpd server pathname	Overrides the **FTP server path** 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). To inform the ***cmuftpd*** daemon to use the FTP client that has SOCKS capabilities, users must start ***cmuftpd*** with parameter **-S**. By default, ***cmuftpd*** does not use the FTP client with SOCKS capabilities. All clients with SOCKS capabilities refer to the */etc/socks.conf* file to navigate the SOCKS firewall. The *socks.conf* 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	Specifies the maximum number of FTP sessions (auto connect and remote connect) that can be running simultaneously in the system. The default is 20. Specify this value using the **Maximum number of current sessions** parameter on the Create a Schedule screen in the Site Administration user interface. If all the remote accounts listed in a single ACD are FTP remote accounts, you cannot set **Sessions** to a value greater than that specified with the FTP daemon **-x** parameter. If the list contains a mix of remote accounts using different protocols, **Sessions** can be effective in limiting the total number of simultaneous sessions for that auto connect to a value greater than the **-x** value for FTP. Unlike Async and Bisync, FTP is not limited by a finite number of physical ports. Each FTP session consumes system resources. If the **-x** 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 **-x** parameter, the following message is posted to stderr: `ERROR: cmuftpd - No of Sessions exceeded MAX_FTP_ SESSIONS (20) limit.` 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 **Requeues** parameter permits the failing session to be requeued for a subsequent attempt. If **Requeues** was set to **0** in the ACD, the session fails without being requeued. If this error occurs when the 21st FTP session is a remote connect, the FTP remote must retry. See the **Times to requeue remote resource field on the Create a Schedule screen in the** Site Administration user interface.
-?|-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 **cmuftpd** 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 *$CMUHOME/cpd/ftp.cpd*.
-c	SSHFTP client pathname	Overrides the SSHFTP **client path** 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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.
-L	Port Listener for SSHFTPD	Specifies the port the SSHFTP server daemon monitors for connections. The default is specified in sshftp.cpd. This can be set using the **Listener Port** 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	*daemon Name*	Overrides the default daemon name of SSHFTP. Daemon names should be 8 characters or less with no spaces.

Parameter	Value	Description
-P	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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 sshftp 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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-s	sshftpd server pathname	Overrides the SSHFTP **server path** parameter specified in the CPD file. It specifies the full path and file name of the SSHFTP server daemon.

Parameter	Value	Description
-x	max SSHFTP sessions	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 **Maximum number of current sessions** parameter on the Create a Schedule screen in the Site Administration user interface. If all the remotes listed in a single ACD are SSHFTP remotes, you cannot set **Sessions** to a value greater than that specified with the SSHFTP daemon **-x** parameter. If the list contains a mix of remotes using different protocols, **Sessions** can be effective in limiting the total number of simultaneous sessions for that auto connect to a value greater than the **-x** value for SSHFTP. Unlike Async and Bisync, SSHFTP is not limited by a finite number of physical ports. Each SSHFTP session consumes system resources. If the **-x** 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 **-x** parameter, the following message is posted to stderr: `ERROR: cmusshftpd - No of Sessions exceeded MAX_SSHFTP_ SESSIONS (20) limit.` 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 **Requeues** parameter permits the failing session to be requeued for a subsequent attempt. If **Requeues** was set to **0** in the ACD, the session fails without being requeued. If this error occurs when the 21st SSHFTP session is a Remote Connect, the SSHFTP remote must retry. See the **Times to requeue remote resource field on the Create a Schedule screen in the** Site Administration user interface.
-?|-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 *$CMUHOME/cpd* 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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-l	debug level	Specifies the debug message level.
-N	daemon name	This parameter is required if you intend to run multiple copies of ***cmubscda***. The ***cmubscda*** 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 **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.

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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-T		Must be specified when using the *rticbscp.exe* 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 */dev/artic,* you must invoke **cmbuscda** with this option. For example: cmubscda -X /dev/artic2.
-?|-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 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 *bisyncc.cpd*.
-d	debugfile	Specifies the debug message output file name.

Command	Parameter	Associated Values
-H	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-I	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	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-?|-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. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-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 **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce 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.setSoTimeout(). The value can be changed by setting the com.sterlingcommerce.ceu.http.listenerTimeout value in the ceuhttpd 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	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-I	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	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-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. *CAUTION*: Use this switch only when instructed to do so by Sterling Commerce Support or Development.
-x	max sessions	Specifies the maximum number of EDIINT sessions that are supported. The default value is 20.

Shutting Down Connect:Enterprise

While individual parts of 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 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 --host	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*

Parameter	Value	Description
-i --immediate		Changes the method Connect:Enterprise uses to shut down the system. Usually, 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 --port	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.
-p --passwd	password	Specifies the value within 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 Connect:Enterprise.
-u --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.
-? --help		Displays the usage message.

Shutting Down Connect:Enterprise Base

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

cmushutdown Format

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

```
cmushutdown
```

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 --host	hostname	Specifies the IP address or host name where the Control daemon is executing. Connect:Enterprise can retrieve this information from one of four sources. The order of resolution is: ◆ The value passed on the command line using the **-H** parameter ◆ The value of the CMUHOST environment variable ◆ The value of the gethostname() system call ◆ The literal value of *localhost*
-i --immediate		Changes the method Connect:Enterprise uses to shut down the system. Usually, 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 --port	portno	Specifies the port the Control daemon monitors. If **-P** 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: ◆ If the value begins with a digit, the value is converted to an integer and the result is used as the control port number. ◆ 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. ◆ If these two tests fail, the default value of 8000 is used.

Parameter	Value	Description
-p --passwd	password	Specifies the value within 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 Connect:Enterprise.
-u --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.
-? --help		Displays the usage message.

Chapter 6

Role-Based Access

This chapter provides information on designing your role-based access system for the Connect:Enterprise 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 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 Connect:Enterprise UNIX Site Administration user interface must be assigned to a role.

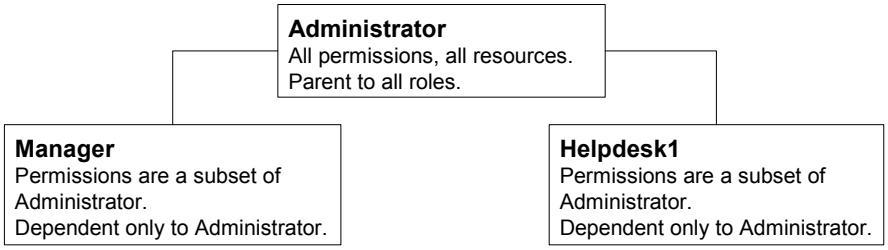
Connect:Enterprise is installed with a single active role: Administrator. The Administrator role has access to all resources and is the parent of all roles that you create. You cannot change anything about the Administrator role. The userID assigned during installation is associated with the Administrator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

You can set up a single-level role-based access system in which roles operate independently of each other. You can also can 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 136 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:

Role Name: **Manager**
Resource Permissions
  Data Management - Modify
  Reports - View
Role Permissions
  None
Accounts Assigned to Role
  user01-mgr
  user02-mgr

Role Name: **Helpdesk1**
Resource Permissions
  Accounts - Administer
  Data - Administer
  Password - Administer
  Policy - View
  Reports - View
  Role-Based-Access - Administer
  Schedule - Administer
  Security - View
  System - View
Role Permissions
  None
Accounts Assigned to Role
  user03
  user04

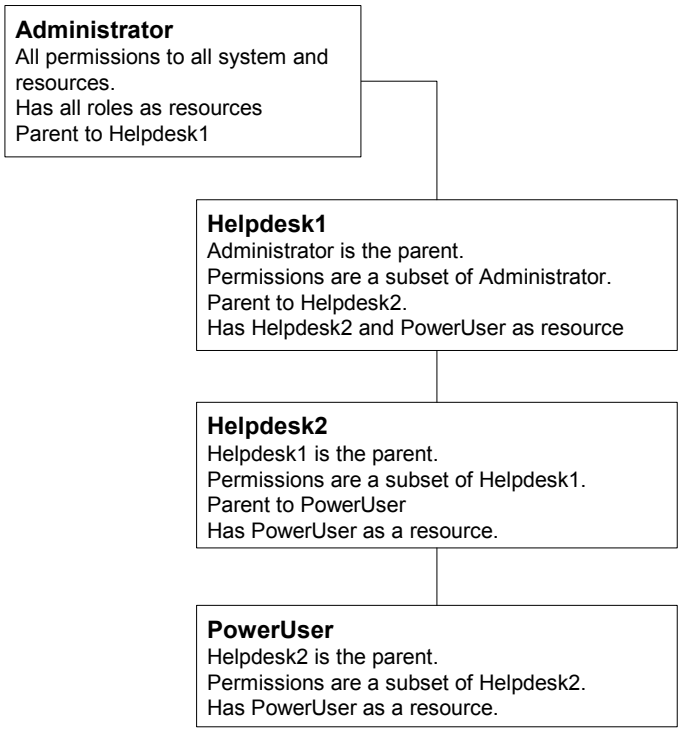
5. Use the **Define Roles** function in the Connect:Enterprise UNIX Site Administration user interface to create the roles and assign accounts to each role.

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-base 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:



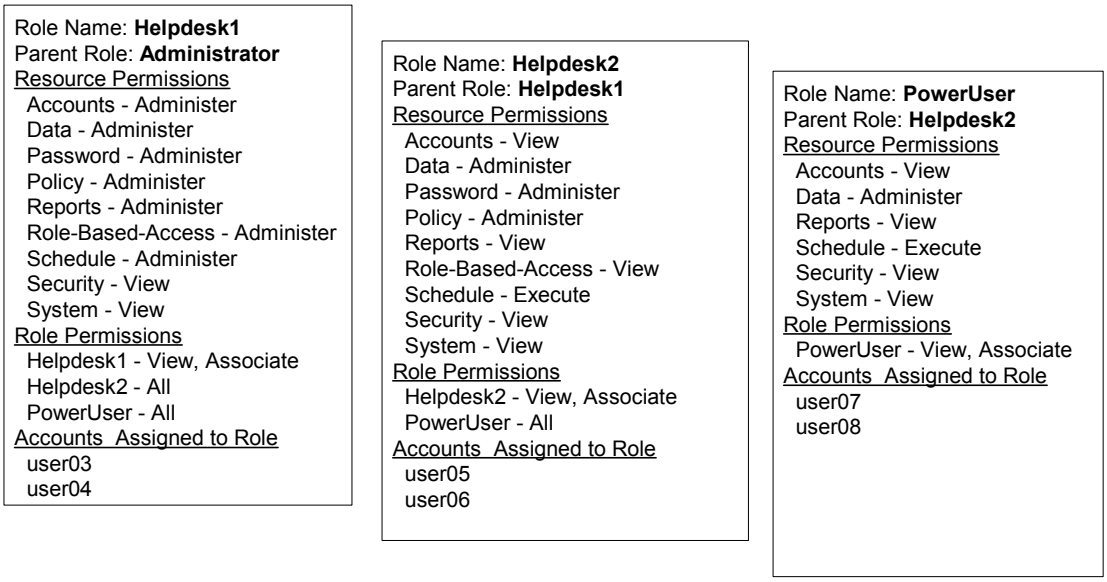
To create a multilevel role-based access system, use the following procedure:

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 136 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 139 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 136 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 139 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 135-step 8 on page 136. Following is an example of what role definitions for a multi-level role-based access system would include:



   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 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.
	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.

Resource	Permission Level	Description
Policy	Administer	Users assigned to the role can create, update, and delete password policies.
Reports	View	Users assigned to the role can generate Connect:Enterprise reports.
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.
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.

Chapter 7

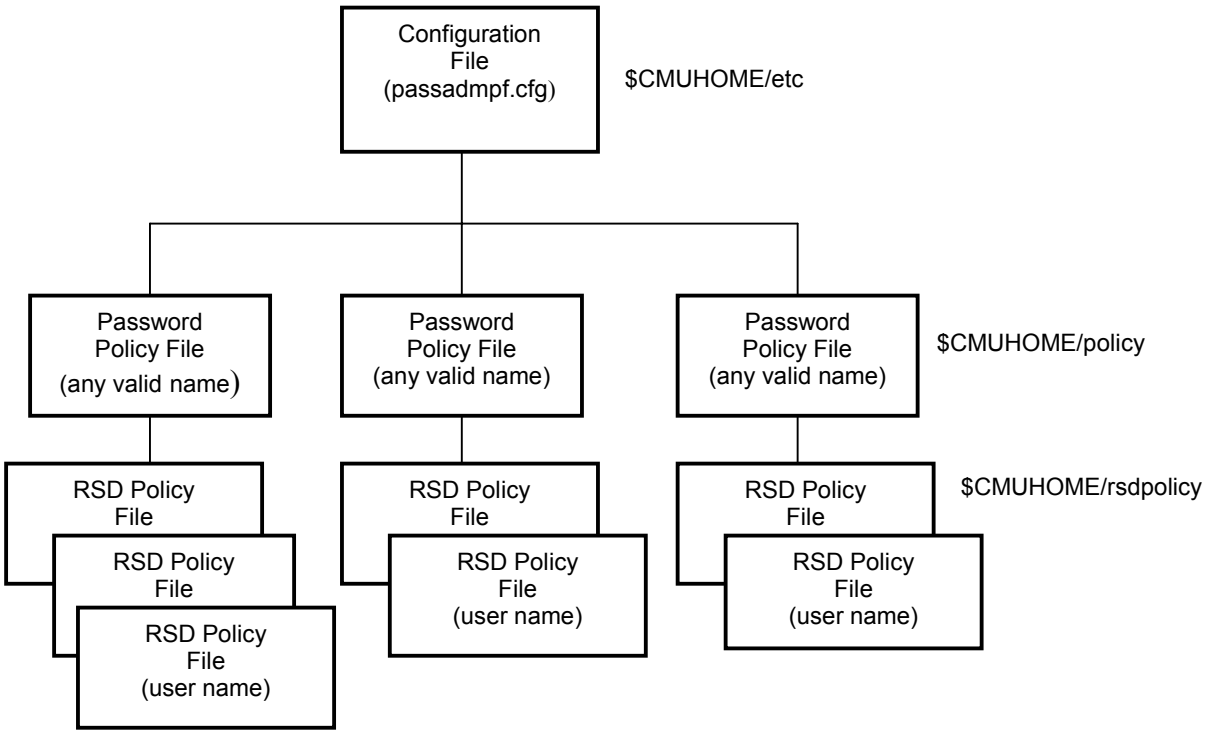
Password Administration

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 Connect:Enterprise 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 Connect:Enterprise Site Administration user interface described in Chapter 1, *About Connect:Enterprise 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: 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. 1 = Optional; If the RSD policy file exists for the user, it is evaluated. 2 = Required; All users who log on to Connect:Enterprise 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 144 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 143) 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 Connect:Enterprise offline password utilities or the 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 Connect:Enterprise utilities or the 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.

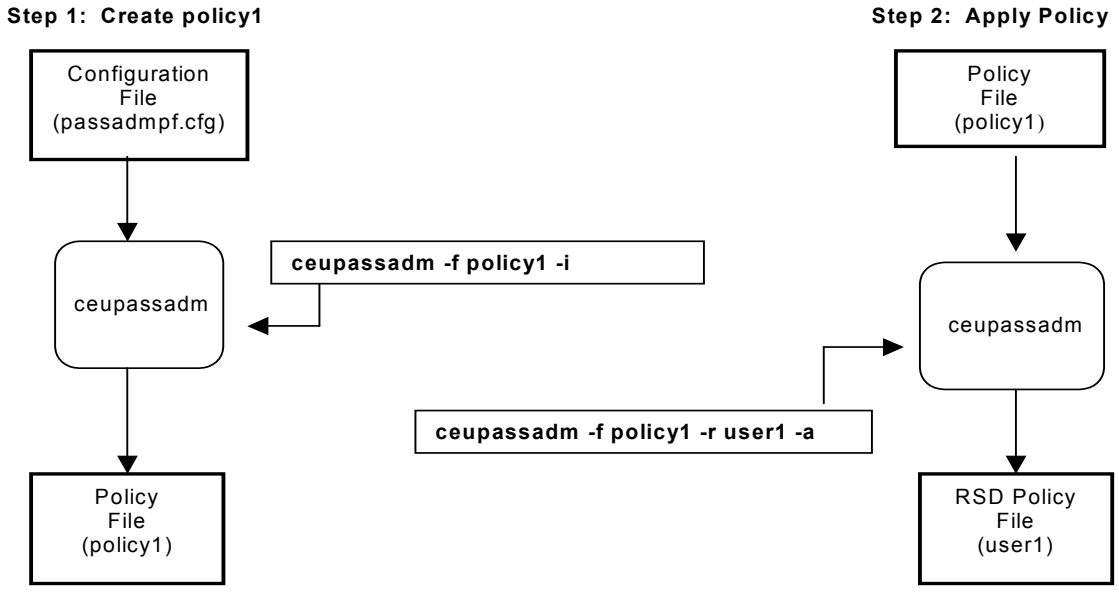
Creating and Maintaining Password Policy Files

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

Command/Utility	Description
ceupassadm	Creates and maintains password policy files and RSD policy files.
ceupassrpt	Displays RSD policy files.
ceupasswd	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 145.

Parameter	Description	Value
-f *filename* --file	Specifies policy file name to process.	Any valid UNIX file name.

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

The following parameters apply only to RSD policy files:

Parameter	Description	Value
-r *rsdpolicy_filename* --rsdpolicy	Specifies the RSD policy file to process.	Any valid RSD policy file name.
-L TRUE | FALSE --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 *nnn* --warning *nnn*	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: *Password will expire in nnn days*.	Valid values are 1–30.
-C TRUE | FALSE --Change	Specifies whether the user must change password at first logon.	Valid values are TRUE or FALSE; default is FALSE.
-S *newpassword* --Specify *newpassword*	Assigns a new password to the account.	Any valid password.
-a --apply	Applies the password policy to the RSD file.	None.
-b *bulk_filename* --bulk *filename*	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. 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 --help	Lists command line options (help).	None.
-x --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
```

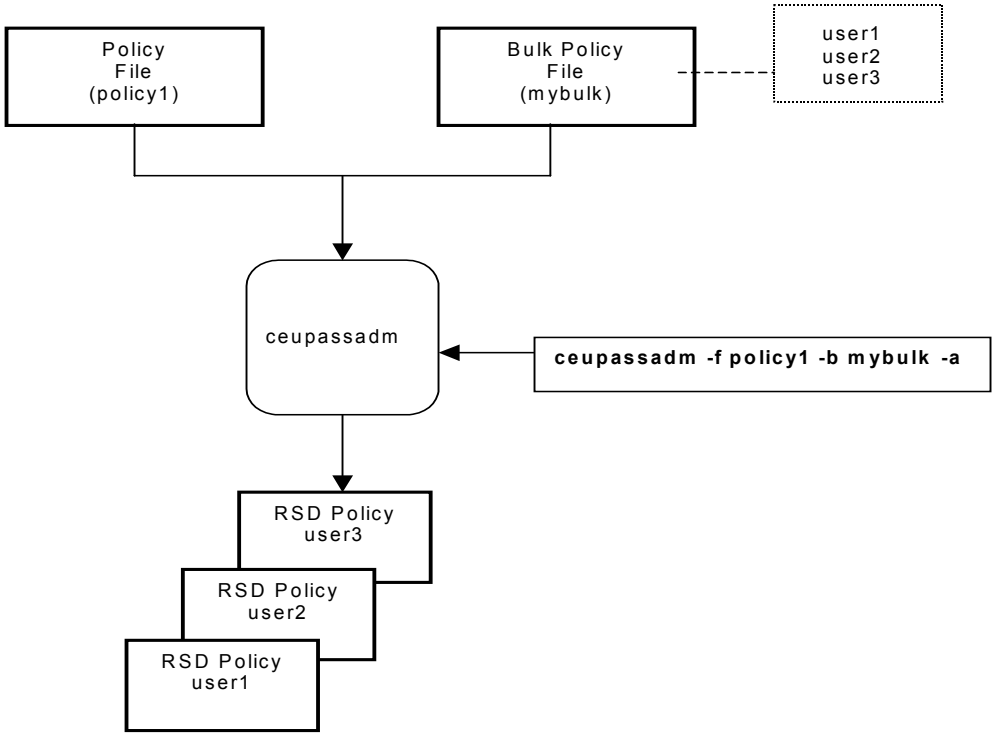
The resulting *policy1* file is:

```
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 *rsdpolicy_filename* --rsdpolicy r*sdpolicy_filename*	Specifies the RSD policy file name.	Required; can be fully qualified or use wildcard character (*).
-e *mm/dd/yyyy* --expiration *mm/dd/yyyy*	Specifies the password expiration date.	Optional; date on or before password expires.

Parameter	Description	Value
-p *pwdpolicy_filename* --pwdpolicy *pwdpolicy_filename*	Specifies the password policy file name.	Optional; password policy that governs this RSD policy.
?,-h --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 Connect:Enterprise 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 *hostname* --Host *hostname*	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 *portno* --Port	Port to connect to for authentication service.	Port number where authentication service is running (optional if CMUPORT is set).
-u userid --**userid**	User ID of person executing **ceupasswd**.	Valid user ID. Required.
-p *password* **--password**	Password of person executing **ceupasswd**.	Current password. Required.
-n *newpassword* **--new**	New password.	New password. Required.
-c *newpassword* **--confirm**	Confirm new password.	New password. Required.
?, -h --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 281 for explanations about the error messages that display in this log file.

Chapter 8

Administrator Commands

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

- Generate and administer the global key used for batch and password encryption (**ceukey**)
- 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 Connect:Enterprise activity (**ceutrace**)

Generating the Global Key (ceukey)

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

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

- *Creating a Global Key* on page 156
- *Encrypting RSD Passwords* on page 157
- *Changing the Passphrase of the Global Key* on page 158.
- *Replacing Your Global Key* on page 158

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 160.

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 157 and step 6 on page 157, move $CMUHOME/keys/key.clear and $CMUHOME/keys/deskey.clear to a secure location. The $CMUHOME/keys directory is not secure.
9. Restart 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 *Connect:Enterprise 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 your created your global key and 3DES global key in *Creating a Global Key* on page 156, this procedure is not neccesary. 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 158, 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 158 and *pathtodesclearkey* is the location of the 3DES clear key from step 1 on page 158.

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 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 *accountname*	Specifies to create a key to associate with an account. The *accountname* is the name of the account (RSD) to create the key for. They key pair is stored as: $CMUHOME/ssh/users/sshftp/*accountname*/id_rsa and $CMUHOME/ssh/users/sshftp/*accountname*/id_rsa.pub. You can specify a different name for the key using the -f parameter or when prompted. If you do not specify this parameter, the public and private keys are stored in the current directory. If you are changing the passphrase of a key, this parameter is required.
-f *path*	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 *filename*	Used with the -e parameter to specify the name of the file to export. Used with the -i parameter to specifies the file to import.

Parameter	Description
-t *type*	Specifies the type of key to create. Valid values are **rsa** and **dsa**. The default is **rsa**.
-b *nnnn*	Specifies the key length in bytes. The default is 1024.
-N *passphrase*	Specifies the new passphrase. Used with -p.
-P *passphrase*	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 Connect:Mailbox for UNIX or Connect:Enterprise 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 *password* --password *password*	Specifies the 1–8 character clear password for an RSD file
-r *rsd file pattern* --rsd *rsd file pattern*	Specifies a set of RSD files for which to encrypt passwords.
-? --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 172 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
-t *{all|acd|rsd|cpd|med|mcd|spd|acl|enc}*	Type of configuration file **Note:** The *enc* option specifies the encrypt.cfg file.
-d *debug_file*	Generates a debug file
-f *cfg_filename*	Specifies a file to be checked
-l *debug_level*	Specifies debug level
-o *output_filename*	Stores all results
-p *{bsca*}- valid for AIX -p {*ftp*|*bsc*|*bscc*|*async*|*sshftp*}- valid for all platforms	Indicates CPD file protocol. The BSCC value is specific to Cleo SYNCcable+ connections. (required for CPD files only)
-v	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 172 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
-C *medfile*	MED file name
-c *ctrldir*	Path of control directory
-D	Generates a debug file
-d *datadir*	Path of data directory
-H *hostname*	Host computer where cmuctld started
-i	Prompts with interactive queries
-n	Specifies diagnostic only
-P *portno*	Port number where cmuctld started
-?	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 173 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 155 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 Sterling Commerce 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 *maxbno*	Maximum batch number
-c *ctrldir*	Path of control directory
-d *datadir*	Path of data directory
-m *meddir*	Path of directory for MED file
-s *minfree*	Minimum free space
-p *prefix*	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 174 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 $CMUHOME is set to the Connect:Enterprise home directory:
ControlDir=$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 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 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 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 Connect:Enterprise.

Tracing Connect:Enterprise Activity

You can use the dynamic tracing command (**ceutrace**) to turn tracing on and off and to set tracing levels without restarting 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 166
- *Daemon Considerations* on page 170
- *Locating Your Trace Files* on page 171
- *Turning Tracing On* on page 166
- *Clearing and Restarting Your Trace Files* on page 172

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 --on	Turn trace on Turns tracing on at the target daemons and displays the current trace settings. 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 --off	Turn trace 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 *hostname* --host *hostname*	Host computer where the control daemon was started.
-P *portno* --port *portno*	Port number where the control daemon was started.
-p *password* --passwd *password*	Connect:Enterprise password
-d *daemon names* --daemon *daemon names*	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: ceutrace –d “FTP*” –on Refer to *Daemon Considerations* on page 170.
-m on|off --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. 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.

Parameter	Description
-f *--filename*	Trace filename prefix 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).
-l *--level*	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. **Note:** Tracing will affect performance. Do not specify levels higher than 10 unless instructed by Sterling Commerce. 0 High level messages and errors only 1–2 Logon / Logoff activity, statistics 3–4 FTP command traffic, simple program logic flow 5–8 One-line inter-process Communication (SIPS) flow, more program flow 9 SIPS records dumped (first 176 bytes) 10–49 More exhaustive debugging 50-98 Full SIPS records dumped 99 All known debug output 100 Full SIPS records dumped (field by field) The Java daemons (cmuhttp, cmuediintd, and cmuadmind) have the following log4j logging levels: =0 off—No logging <=5 sparse—Errors only <=9 moderate—Errors and warnings only <=50 detailed—Includes informational <=99 verbose—Includes trace data
-a *--account*	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. For example, to trace the remotes RMT1, RMT2, … RMT10, but not RMTTEST, turn on FTP tracing for all but RMTTEST by specifying: ceutrace –d FTP –on –account “RMT*,!RMTTEST”

Parameter	Description
-L *--listname*	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. 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: ceutrace –d FTP –on –L “LIST*,!*10*”
-D --delimited	Specifies to return pipe delimited output.

2. Enter the **ceutrace** command similar to the following example, using the parameters and values determined in step 1 on page 166. See *cmuinit Example* on page 174 for additional examples using the **ceutrace** command.

```
ceutrace -on -d “FTP*” -m -l9
```

3. The status of each daemon is displayed. Following is an example:

```
              Command Line Parameters:
                        ceutrace
Name         SID      Trace  Level   Filename
                      Status         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 171.

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	cmuadmind, admin daemon
EXITS	cmuexitd, exits server
SYSLOG	cmulogd, log server
ACD	cmuacd, autoconnect server

With ceutrace, each daemon is managed differently by 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

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)	*<prefix>*.SLV.*<pid>*
Async Daemon (cmuasyd)	Trace files for remote connect sessions are initially created as: *<prefix>.<port-name>.<pid>*. Once a session is established the file is renamed to *<prefix>.<port-name>.<account>.<session-ID>.<pid>*
FTP Daemon (cmuftpd)	For remote connections: *<prefix>.svr.<account>.<sessionID>.<pid>* For autoconnects: *<prefix>*.clt.*<account>.<sessionID>.<pid>*
SSH Daemon (cmusshftp)	*<prefix>.<direction>.<function>.<account>.<sessionID>.<pid>*
Bisync Daemon (cmubscda, cmubscdc)	Trace files for remote connect sessions are initially created as: *<prefix>.<port-name>.<pid>*. Once a session is established the file is renamed to *<prefix>.<port-name>.<account>.<session-ID>.<pid>*

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 166.
- If you do not want to save old trace files, reissue the trace command using *Turning Tracing On* on page 166.

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
ACPRIORITYLEVEL = 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: 01/27/04       Connect:Enterprise UNIX n.n.nn
Time: 14:59:33       Validate Mailbox Database, Rebuild Indices


Time: 14:59:33  Now validating database and rebuilding index files.

Time: 14:59:34  Index rebuild is complete. Getting record counts.

Time: 14:59:34  1529 active records in database. Highest batch number: 1537

Time: 14:59:34  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       Connect:Enterprise UNIX n.n.nn
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
```

Chapter 9

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 requeued 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
-s *rcs*|*rcd*|*acs*|*acd*|*acq*|*off* --type *rcs*|*rcd*|*acs*|*acd*|*acq*|*off*	**Specifies Report type.**
-? --help	Lists command line options (help).
-B *[CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm* --Begin *[CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm*	Selects batches created on or before date.

Parameter	Description
-c --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 --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]yymmdd|nnn[:hhmm|/hhmm]|[hhmm]* --from *[CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm]*	Selects batches created on or after date.
-F *log filename* --name *log filename*	Specifies name of log file.
-i *remotename* --rmt *remotename*	Specifies that -srcd or -srcs is required.
-L *listname* --list *listname*	Specifies auto connect (schedule) list name.
-M --more	Posts output messages one screen at a time.
-N *number* --files *number*	Specifies number of log files to use.
-p *pathname* --path *pathname*	Specifies location of logacct.dat files.
-r --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* --status *f|s|a*	Returns the status.
-t *[CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm]* --to [*CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm]*	Selects batches created on or before date.
-T *[CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm]* --TO [*CC]yymmdd|nnn[:hhmm|/hhmm]|[hhmm]*	Selects batches ending on or before date.
-v --verbose	Displays session activity.
-X *nnnn* --cols *nnnn*	Specifies columns available for screen display.
-Y *nnnn* --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|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|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|||||
```

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
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. 10 = Remote connect records 20 = Auto connect records 30 = Queued auto connect records 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 Remote session information Remote session end Auto connect session start Auto connect remote start Auto connect information Queued auto connect Offline command	Start date and time.
6	All	Connect:Enterprise session number. Valid for all record types.
7	All	Message type. Indicates the type of information in the record: 1 = Remote connect start 2 = Auto connect remote start 3 = Remote information 4 = Offline information 5 = Remote end 6 = Auto connect end
8	Remote session information Remote session end Auto connect information Auto connect remote end Auto connect session end Offline command	End date and time.

Field Position	Valid for Records	Description
9	Auto connect information Auto connect remote end	Sub message type. For auto connect information, this is the remote function code: 1 = Add 2 = Request 3 = Directory 4 = Delete 5 = NOOP For auto connect remote end records, this is the auto connect status.
10	Remote session information Remote session end Auto connect information Auto connect session end Queued auto connect Offline command	Status code for the remote command. Values are noted in *Appendix A, Error Messages*, in the *Connect:Enterprise Installation and Administration Guide*.
11	Remote session information Queued auto connect	Function code: 1 = Add 2 = Request 3 = Directory 4 = Delete 5 = NOOP
12	Remote session start Auto connect remote start	Protocol 1 = TCP/IP (offline) 2 = Async 3 = FTP 4 = BSC 5 = Secure FTP
13	Remote session information Auto connect information 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.
14	Remote session information Auto connect information Offline command	Size in bytes of the batch affected by the command. Valid for Accurately reports all file sizes.
15	Remote session information Auto connect information Offline command	Batch number assigned by Connect:Enterprise.

Field Position	Valid for Records	Description
16	Remote session information Remote session end Auto connect information Auto connect session end Offline command	This parameter has different meanings for different record types as follows: For remote session end, this is the number of batches added during the session. For auto connect session end, this is the number of batches added (received). For offline commands, this is the offline function code: 0 = Add 1 = Extract 2 = Status 3 = Deleted 4 = Erase
17	Remote session information Remote session end Auto connect information Auto connect session end	For remote session end, this is the number of batches requested during the session. 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 Auto connect session end	The number of batches deleted
20	Remote session end Auto connect session end	The number of batches added without $$ADD.
21	For future use	
22	Remote session information Auto connect remote start Auto connect information Auto connect remote end 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. 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.
23	Remote session information Auto connect session start Auto connect information Auto connect session end Queued auto connect Offline command	For remote session information and auto connect information, this is the batch ID assigned by Connect:Enterprise.

Field Position	Valid for Records	Description
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 Auto connect remote start Auto connect information	For the business process (BP) protocol, this is the GIS workflow ID and the GIS status URL. 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: 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           Connect:Enterprise 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 GIS account, this column shows the GIS 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, *Error Messages*.
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        Connect:Enterprise 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. Convert Auto Connect Failure Codes from decimal to hexadecimal and search for a description in Appendix A, *Error Messages*.

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 Connect:Enterprise and when each remote site command was processed by Connect:Enterprise.

```
Date:  mm/dd/yy          Connect:Enterprise 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    nnnnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  hh:mm:ss   nnn     xxx   nnnnnnn   nnnnn   nnnnn    nnnnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  hh:mm:ss   nnn     xxx   nnnnnnn   nnnnn   nnnnn    nnnnn
```

Each Remote Connect Detail Report contains the following information:

Column	Description
Remote	The name of the remote site that connected to 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, *Error Messages*.
Func	The 3- or 4-byte field that describes the event being reported. Function types are: CON-The remote site connected to Connect:Enterprise. DISC-The remote site disconnected from Connect:Enterprise. ADD-The remote site sent an $$ADD or put command. REQ-The remote site sent a $$REQUEST or get command. DEL-The remote site sent a $$DELETE or del command. DIR-The remote site sent a $$DIRECTORY or dir command. 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).
BpId	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        Connect:Enterprise 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 Connect:Enterprise.
Start	The date and time the remote site connected to 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 **$$ADD** or **put** commands.
woA	The number of batches of data that were successfully added *without* using the **$$ADD** or **put** command.
Req	The number of batches that were transmitted in response to **$$REQUEST** or **get** commands.
Dir	The number of $$DIRECTORY or **dir** commands issued by the remote site.
Del	The number of successfully-processed **$$DELETE** or **del** 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 requeued auto connect and the specific remote site where the connection was requeued.

```
Date:  mm/dd/yy      Connect:Enterprise UNIX      Page 0001
Time:  hh:mm:ss          Report Utility


Command Line Parameters:
     cmureport
     -sacq


List      Start              Remote    Resource  Status


xxxxxxxx  yy/mm/dd-hh:mm:ss  xxxxxxxx  xxxxxxxx  nnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  xxxxxxxx  xxxxxxxx  nnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  xxxxxxxx  xxxxxxxx  nnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  xxxxxxxx  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 requeued.
Remote	The remote site where the requeue 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, *Error Messages*.

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      Connect:Enterprise 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  nnnnnnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  hh:mm:ss  xxx      xxxxxxxx   nnnnnn  nnnnnnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  hh:mm:ss  xxx      xxxxxxxx   nnnnnn  nnnnnnn


xxxxxxxx  yy/mm/dd-hh:mm:ss  hh:mm:ss  xxx      xxxxxxxx   nnnnnn  nnnnnnn
```

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 **ADD** or **EXTRACT**, 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 Connect:Enteprise UNIX command line utilities, the as2report utility does not allow spaces between a parameter and its values.

Parameter	Description
-byyyymmdd[:hhmm]|hhmm --begin yyyymmdd[:hhmm]|hhmm	Specifies the begin date and time the messages were transferred.
-e*yyyymmdd[:hhmm]|hhmm* --end *yyyymmdd[:hhmm]|hhmm*	Specifies the end date and time the messages were transferred.
-f*['] from name ['] * --from *['] from name ['] *	Specifies the from AS2 identifier of the AS2 contract.
-h --help	Print usage information.
-m*column delimiter* --delimit *column delimiter*	Specifies the delimiter to use to separate columns. If the delimiter is not specified, column fields will be printed fixed width. For more informatio about the -m parameter, refer to *Displaying Pipe-Delimited AS2 Reports* on page 189.
-n*['] contract ID ['] * --contract *['] contract ID ['] *	Specifies the contract ID associated with the AS2 transfer.

Parameter	Description
-r*inbound*|*outbound*|*both* --direction *inbound*|*outbound*|*both*	Specifies the direction of the AS2 transfer from Connect:Enterprise.
-s*success*|*failed*|*pending*|*all* --status *success*|*failed*|*pending*|*all*	Selects the status the AS2 message.
-t*['] to name ['] * --to *['] to name ['] *	Specifies the to AS2 identifier of the AS2 contract.
-x --xml	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"|" -byyyyymmdd[: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.M
D"|"batch.PL"|"hostname1.com-1bdb58-102fee47e89--8000@hostname2.com"|"remote"|"local
"|"hostname1.com-1bdb58-102fee47e89--7fffremote@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

Field Position	Description	Example Field
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--7fffscooby@hostname2.com"
20	Disposition	"processed"
21	Disposition modifier. This field only has a value if the MDN is negative.	“”

Chapter 10

Configuring Secure FTP

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. 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 Connect:Enterprise Secure FTP, both the sending and receiving sites must have FTP software that has SSL capabilities.

Connect:Enterprise Secure FTP Features

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 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 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.

Connect:Enterprise Secure FTP Client-Server Session

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.

Connect:Enterprise Secure FTP enables CSR generation with the **cmusslgencsr** command. 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.

Connect:Enterprise Secure FTP enables server authentication with the **cmusslverify** command., See the *Connect:Enterprise 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 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 immeditaely 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. 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.
4. Decide what **Cipher Suites** to use for your remote sites.

   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 Connect:Enterprise host and other Connect:Enterprise or 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: Connect:Enterprise Command Line Client (Secure FTP) and Connect:Enterprise Secure Client cannot specify cipher suites, only cipher strength.

   The following cipher suites are supported by Connect:Enterprise Secure FTP:

Strength	Ciphers
Strong	SSL_RSA_WITH_3DES_EDE_CBC_SHA SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_RC4_128_MD5 SSL_RSA_WITH_DES_CBC_SHA
Export suites	SSL_RSA_EXPORT_WITH_RC4_40_MD5 SSL_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
Clear text with certificate suites	SSL_RSA_WITH_NULL_SHA SSL_RSA_WITH_NULL_MD5

5. 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.
6. Decide what your clear channel control (CCC) policy will be. The following table describes your options.

Strength	Ciphers
SSL server CCC policy	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. Disallowed = Default. CCC is not attempted. Required = CCC must be accepted for the session. Optional = CCC is attempted. If rejected, the session remains connected and encrypted.
SSL client CCC policy	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. Disallowed = Default. CCC is not attempted. Required = CCC must be accepted for the session. Optional = CCC is attempted. If rejected, the session remains connected and encrypted.

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) and Thawte (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 Connect:Enterprise base installation. If you have already installed 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 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 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 Connect:Enterprise UNIX, Connect:Mailbox for UNIX, Connect:Enterprise Command Line Client (Secure FTP), or Connect:Enterprise Client for 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 *Connect:Enterprise 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 Connect:Enterprise Secure FTP transfers.

Chapter 11

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 Connect:Enterprise UNIX SSH server support SFTP and SCP clients. Use the information in this appendix to configure communication between Connect:Enterprise UNIX and SSHFTP clients.

Configuring Connect:Enterprise SSHFTP 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 Connect:Enterprise UNIX server	Connect:Enterprise 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 Connect:Enterprise SSHFTP 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
Connect:Enterprise only performs password authentication.	Password authentication = Yes Public key authentication = No
Connect:Enterprise only performs public key authentication.	Password authentication = No Public key authentication = Yes

If you want this authentication routine	Set this in the communication definition
Connect:Enterprise first attempts public key authentication. If public key authentication fails, Connect:Enterprise attempts password authentication.	Password authentication = Yes 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 200 through step 4 on page 201.

Chapter 12

Configuring AS2

This chapter provides information on using Connect:Enterprise 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 Connect:Enterprise 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 Connect:Enterprise 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.

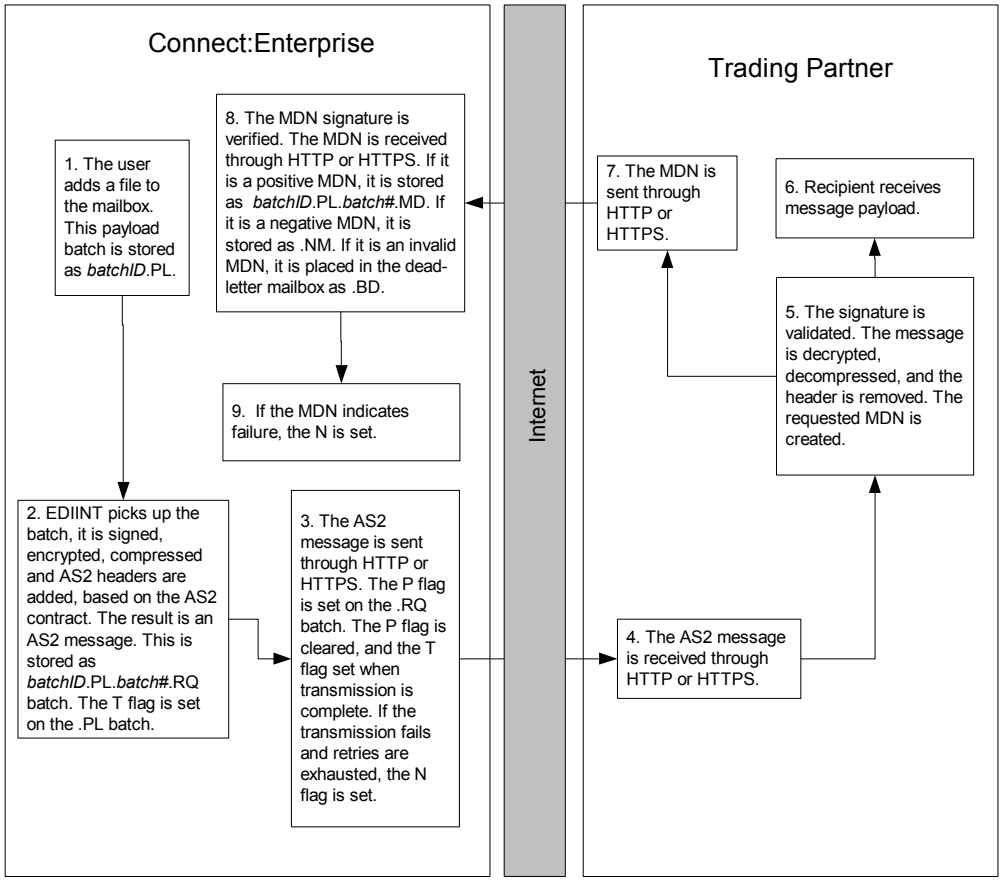
Implementing AS2 requires you to agree with your trading partner on security options, including signing, encryption, and Message Delivery Notification (MDN) options. You will also need to exchange AS2 identifiers, certificates for S/MIME and SSL (HTTPS) and information about the HTTP URLs and ports that each of you will be using for the exchange.

The following diagrams illustrates how 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 Connect:Enterprise to a Trading Partner

The following diagram illustrates the process when sending batches from 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.

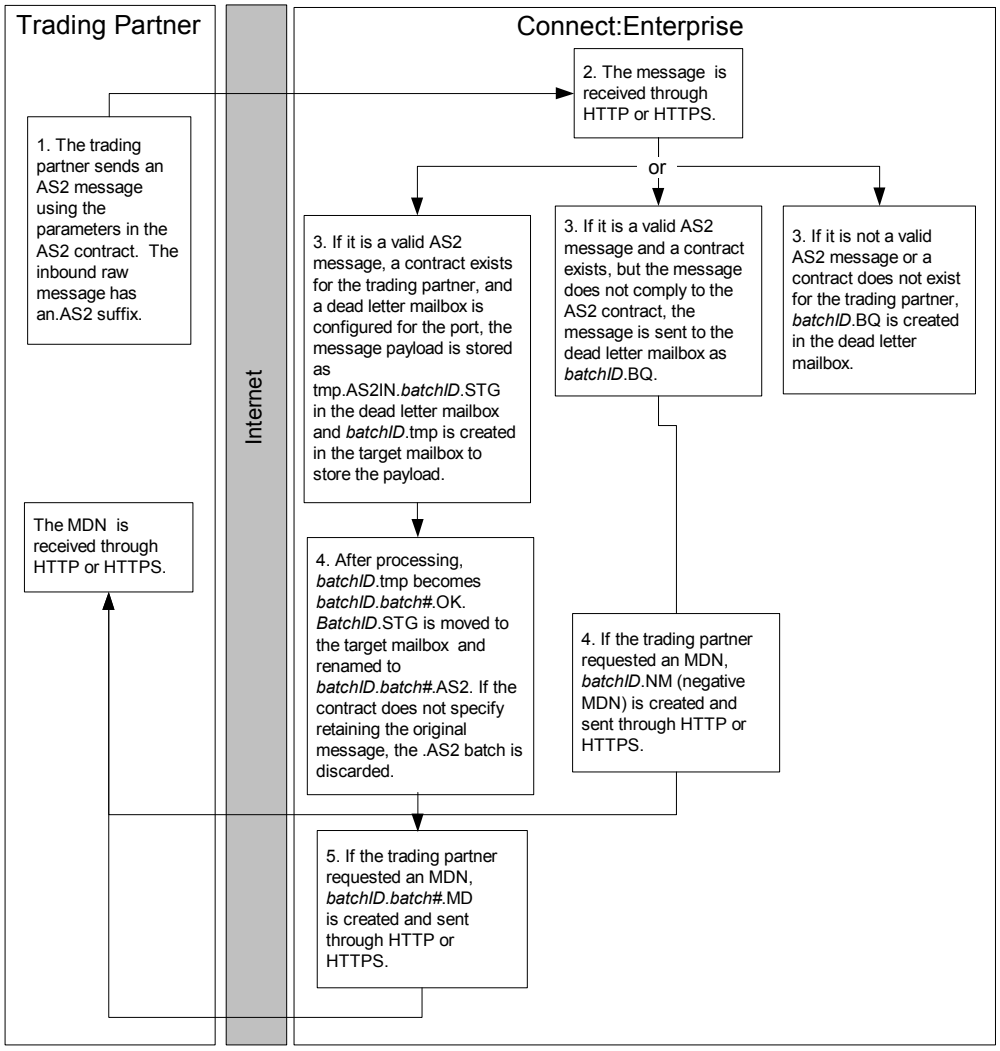


Note: Not all batches referred to in these diagrams are always created. If the "retain original message in recipient mailbox" option is not enabled, the .AS2 batch is not saved for inbound messages and the .MD batch is not saved for outbound messages.

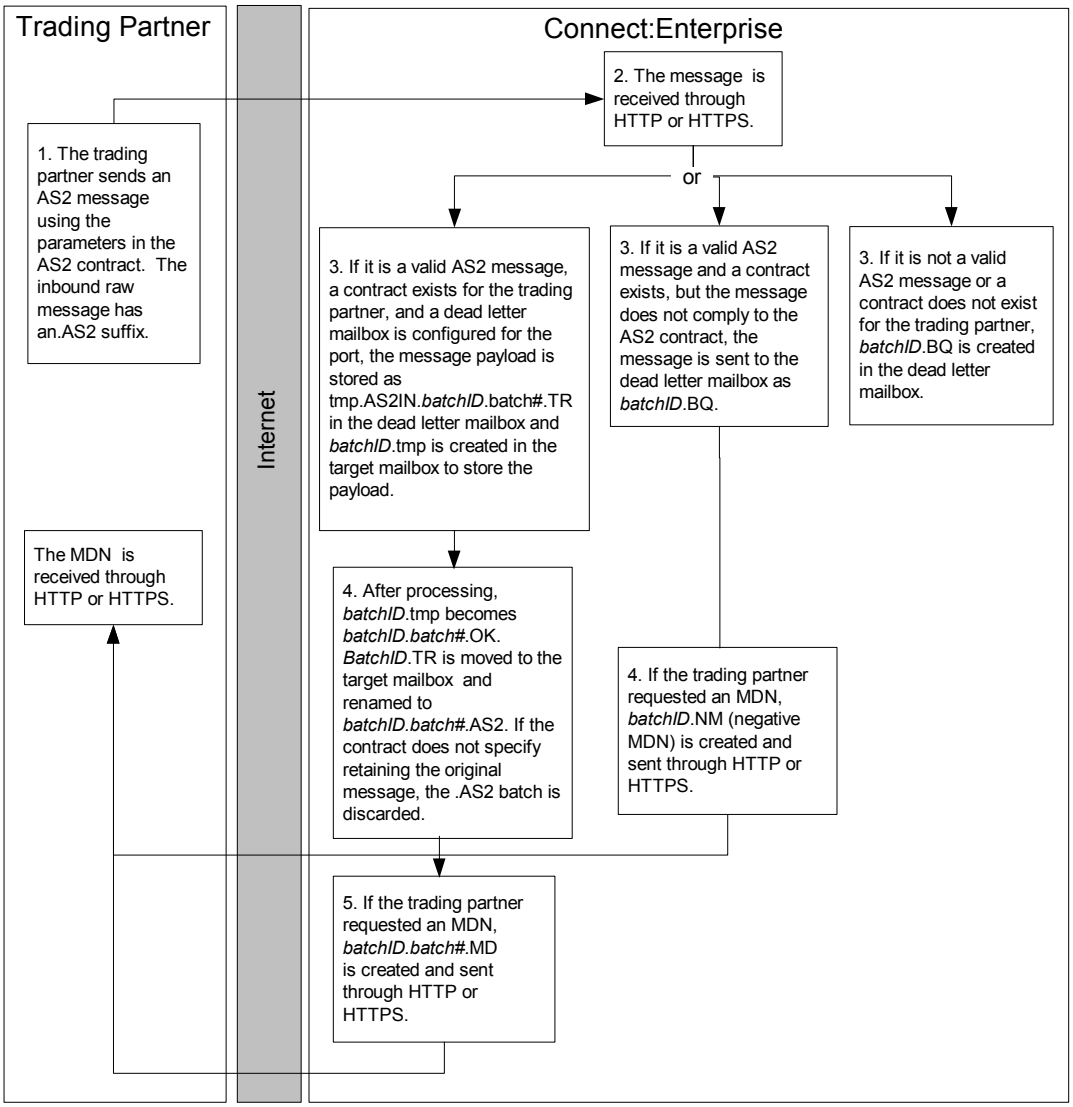
Receiving AS2 Messages from a Trading Partner

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 Connect:Enterprise 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:

```
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) Unix(TM)
version n.n.nn  Customization

This customization procedure sets up AS2 for Connect:Enterprise 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 "/opt/java1.4/jre/bin/java" to configure for AS2


Created script: /data/newsftp/ceunix/javalib/cmuhttpd

Created script: /data/newsftp/ceunix/javalib/cmuediintd

Created script: /data/newsftp/ceunix/javalib/as2report

Created script: /data/newsftp/ceunix/javalib/as2delete

Created script: /data/newsftp/ceunix/as2/AS2-Configuration.xml
AS2 Customization Completed
```

2. Start the HTTP daemon (**cmuhttpd**) and the EDIINT daemon (**cmuediintd**). Refer to Chapter 5, *Starting and Stopping Connect:Enterprise*, for more information.

Changing the Java Version for AS2

If you need to change the Java version that AS2 uses, perform the following procedure.

1. Navigate to the $CMUHOME/etc directory and run the **java_check** utility. Following is an example of the output.

```
$CMUHOME/etc > java_check

Searching for Java...


******************************************************
Select the appropriate Java interpreter program.

Contact your System Administrator if you are unsure
about the appropriate selection.
******************************************************

0 = User enters the absolute path to Java.
1 = version 1.3.1.07     at /opt/java1.3/bin/java
2 = version 1.3.1.07     at /opt/java1.3/jre/bin/java
3 = version 1.4.0.02     at /opt/java1.4/bin/java
4 = version 1.4.0.02     at /opt/java1.4/jre/bin/java
Select [0-4]: 4
```

2. Type the number corresponding to the Java version you want to use and press **Enter**.
3. Run the **as2cust** utility. This step updates the AS2 configuration file. Following is an example of the output.

```
$CMUHOME/etc > as2cust
================================================================================
Sterling Commerce, Inc.,(TM) Connect:Enterprise(TM) Unix(TM)
version n.n.nn  Customization

This customization procedure sets up AS2 for Connect:Enterprise 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 "/opt/java1.3/jre/bin/java" to configure for AS2


Created script: /data/newsftp/javalib/cmuhttpd
Created script: /data/newsftp/javalib/cmuediintd
Created script: /data/newsftp/javalib/as2report
Created script: /data/newsftp/javalib/as2delete

An existing AS2 configuration file has been found and will not
be overwritten or modified.
The file path is: /data/newsftp/as2/AS2-Configuration.xml

AS2 Customization Completed
```

4. You must restart the HTTP daemon (**cmuhttpd**) and the EDIINT daemon (**cmuediintd**). Refer to Chapter 5, *Starting and Stopping 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 Connect:Enterprise 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: None = Default Strong = Allow only cipher suites with greater than 40-bit encryption. All = Allow strong and weak cipher suites. Weak cipher suites use 40-bit encryption. Custom = Use specific cipher suites. 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 Connect:Enterprise 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
What your trading partner needs from you	
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: http://*hostname*:*port*/as2/*mailbox_ID*/*batch_ID* where *hostname*, *port*, and *mailbox_ID* identify where you want your trading partner to send to and *batch_ID* identifies the name they must give the batch they are sending. If it is a secure port, this URL must begin with https://.
What you need from your trading partner	
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.

Information Required	Description
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
What your trading partner needs from you	
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: None = Default Strong = Allow only cipher suites with greater than 40-bit encryption. All = Allow strong and weak cipher suites. Weak cipher suites use 40-bit encryption. Custom = Use specific cipher suites. 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.
What you need from your trading partner	
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.
Cipher strength for SSL	Cipher strength to be used for SSL. Options are: None = Default Strong = Allow only cipher suites with greater than 40-bit encryption. All = Allow strong and weak cipher suites. Weak cipher suites use 40-bit encryption. Custom = Use specific cipher suites. If you select Custom, you must specify the cipher suites.

Information Required	Description
Common name validation	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: Host name DNS name Other (specify)

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
What your trading partner needs from you	
Signing certificate file	Signing certificate to authenticate messages that you send.
What you need from your trading partner	
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
What your trading partner needs from you	
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 encrypt messages to send to you.
What you need from your trading partner	
Exchange algorithm	Exchange algorithm that your trading partner requires you to use when encrypting messages.

Information Required	Description
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
What you need from your trading partner	
MIME type/subtype	Specific MIME type/subtype your trading partner requires, if any.
Compress message	If your trading partner requires you to compress message.
What you need to decide for your local site	
Port to receive asynchronous MDN	Port available to receive asynchonous 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.

Chapter 13

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 Connect:Enterprise implementation of WebDAV allows you to exchange data with Connect:Enterprise using Windows in the same way that you would any directory structure. You can also use any WebDAV client available with UNIX operating systems.

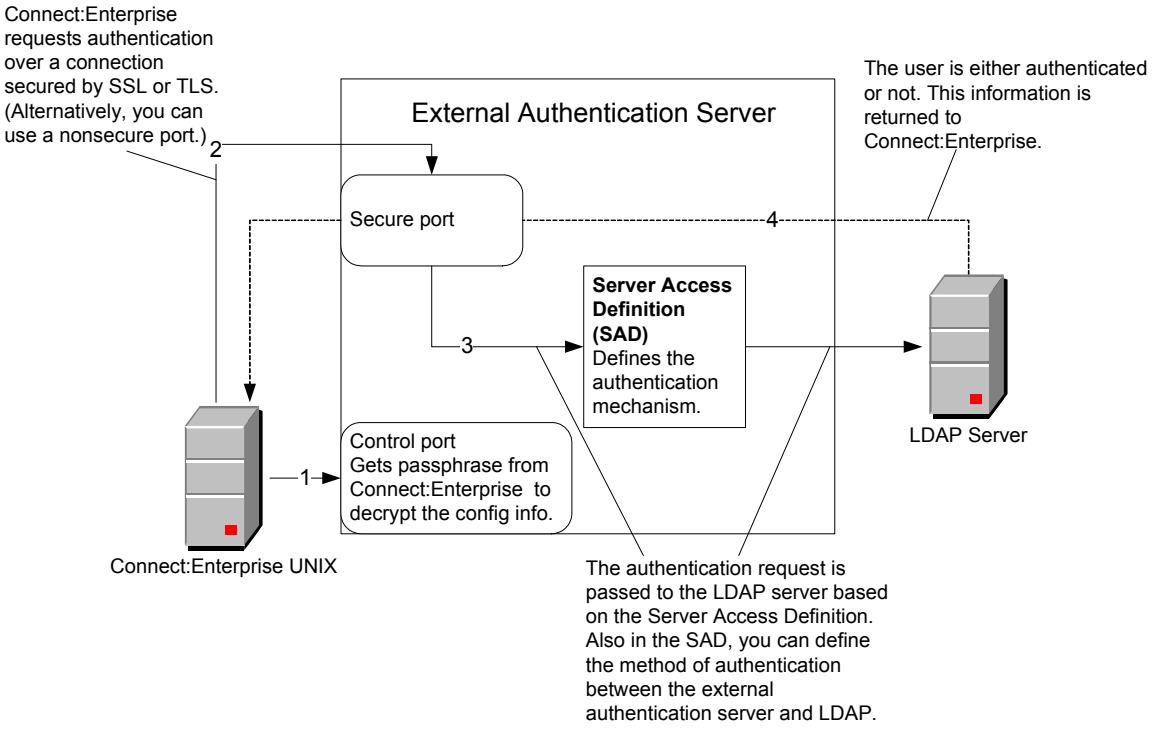
To configure the Connect:Enterprise WebDAV, you only need to configure the HTTP port for WebDAV. Use the Define Communications function of the Connect:Enterprise UNIX Site Administration user interface to set up the WebDAV server. Information on Configuring a WebDAV port are in the Help for the Site Administration User Interface. The initial installation of the 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.

Chapter 14

Configuring the External Authentication Service

The external authentication service that is part of Connect:Enterprise serves as a proxy between 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 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 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 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 Connect:Enterprise and the external authentication service, refer to *Start Connect:Enterprise and the External Authentication Service* on page 224 and *Define the Server Access Definition* on page 228.

Configuring the SSL Credentials for Connection

If you plan to use a secure connection between 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 221 because the certificate and the truststore password must be the same.

1. Type the following command to change the encryption passphrase:

```
changepassphrase.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
keytool	Invokes the keytool utility.
-storepasswd	Instructs keytool to change the password.
-v	Instructs keytool to use verbose output.
-new *newpassword*	Specifies the new password for the keystore.
-keystore *keystore_path*	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 *password*	Specifies the current password of the keystore file. The initial value is *password*.

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
keytool	Invokes the keytool utility.
-storepasswd	Instructs keytool to change the password.
-v	Instructs keytool to use verbose mode.
-new *newpassword*	Specifies the new password for the truststore.
-keystore *truststore_path*	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 *changeit*	Specifies the current password of the truststore file. The initial value is *changeit*.

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 219 and step 6 on page 219:

```
sslinfotool.sh -p=passphrase -w=newkeystorepassword -W=newtrustorepassword
```

The following table describes the command elements:

Element	Description
sslinfotool.sh	Invokes the sslinfotool.sh
-p=passphrase	Specifies the passphrase for the external authentication server you changed in step 1 on page 219.
-w=newkeystorepassword	Specifies the new keystore password you changed in step 5 on page 219.
-W=newtrustorepassword	Specifies the new truststore password you changed in step 6 on page 219.

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 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
keytool	Invokes the keytool utility.
-genkey	Instructs keytool to generate a certificate.
-alias *alias_name*	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. You will also need this information when you *Enable the Secure Access Accepter* on page 226.
-keyalg *alg_type*	Specifies the type of algorithm used to create the key. This value must be RSA.
-keystore *keystore_path*	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 *password*	Specifies the password of the keystore file. Use the value you specified in step 5 on page 219.

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 Connect:Enterprise

Use the following procedure to export the signed external authentication service certificate to 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
keytool	Invokes the keytool utility.
-export	Instructs keytool to export the certificate.
-alias *alias_name*	Specifies the name of the certificate you created in *Create a Key/Certificate for the External Authentication Service* on page 221.
-keystore *keystore_path*	Specifies the path and file name of the key store file. $CMUHOME/externalauth/IDMB/conf/system/keystore is the default. If you use a value other than the default, you must update the sslinfo.xml with the new path and file name using the sslinfotool.sh script.
-storepass *password*	Specifies the password of the keystore file.
-file *$CMUHOME*/spd/*filename*	Specifies the path and filename where you want to export the certificate to. The path will always be $CMUHOME/spd.
-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 Connect:Enterprise

If you already have a key/certificate for Connect:Enterprise, this procedure is not neccesary. If you do not already have a key/certificate for Connect:Enterprise, you can use Sterling Commerce 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 Connect:Enterprise.

1. Navigate to the $CMUHOME/spd directory.
2. Use the following command to create a certificate for 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 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 Connect:Enterprise Certificate to the External Authentication Service Truststore

Use this procedure to import the Connect:Enterprise CA certificate to the external authentication service. It will be used to authenticate the 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
keytool	Invokes the keytool utility.
-import	Instructs keytool to import a certificate to the keystore.
-keystore *truststore_path*	Specifies the path and file name of the trust store file. The default is $CMUHOME/externalauth/IDMB/conf/system/truststore.
-storepass *password*	Specifies the password of the truststore file.
-file *certificate*	Specifies the location of the public certificate to import. If you used *Create a Key/Certificate for Connect:Enterprise* on page 223, this certificate is located in $CMUHOME/spd/cert.txt. 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 Connect:Enterprise and the External Authentication Service

Use the following procedure to start Connect:Enterprise and the External Authentication Service:

1. Start 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 219.

Create and Identify a Security Definition for the External Authentication Service

Use the following procedure to create a security definition to define the 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 *Export the External Authentication Service Certificate to Connect:Enterprise* on page 222.
Key certificate file	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 Connect:Enterprise authentication is used. Specify Yes or RSD to use the external authentication service.	No = Default; use Connect:Enterprise authentication. Yes = Use external authentication. RSD = Authentication method is determined by the account definition.

Parameter	Description	Valid Value
External auth port	Specifies the port that the external authentication service listens on.	Any port between 1-65535. The default is 61365.
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 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 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 225.	Any valid security definition.

7. Click **Save**.

Enable the Secure Access Accepter

Use the following procedure to define the external authentication side of the secure connection from Connect:Enterprise.

1. Using the Site Administration user interface, click **Define Access Accepter**.
2. Select **Secure** from the list and click **Edit**.

3. Set the following parameters:

Parameter	Value
Accepter enabled	Enable
Port	Port number of the External Auth Secure Port in step 6 on page 225
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 *Create a Key/Certificate for the External Authentication Service* on page 221.
Keystore file	Path and file name of the keystore file. The default is *$CMUHOME*/externalauth/IDMB/conf/system/keystore.
Keystore password	Password to the keystore.
Truststore file	Path and file name of the truststore file. The default is *$CMUHOME*/externalauth/IDMB/conf/system/truststore.
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 Connect:Enterprise using **ceushutdown**.
2. Start 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 219.
4. Using the Site Administration user interface, click **Define Access Accepter**.
5. If Secure is available in the LDAP accepter name list, the secure connection between 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 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 Connect:Enterprise, 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 Accepter** on the navigation panel.
2. Select **NonSecure** from the list and click **Edit**.
3. Disable **Accepter 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 Connect:Enterprise, use the procedure detailed in step 5 on page 219. 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.
-storepasswd	Instructs keytool to change the password of a certificate.

Element	Description
-alias	Instructs keytool that the text that follows is the alias of the certificate to change.
certalias	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.
certpassword	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.
newcertpassword	New password of the certificate.

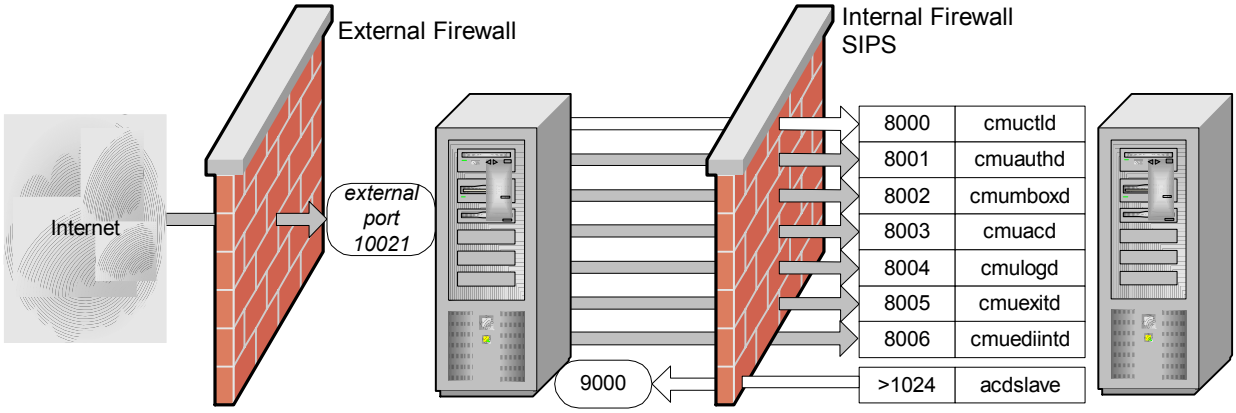
Chapter 15

Running Protocol Daemons on Remote Servers

Connect:Enterprise allows you to run a protocol daemon on a different server than your 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 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 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 Connect:Enterprise server complies with your network security policy.



When 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 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 Connect:Enterprise Components Running on Different Computers* on page 264).

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 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, Connect:Enterprise allows you to run the following daemons from a remote server:

- FTP (cmuftpd)
- SSH (cmusshftpd)
- HTTP (cmuhttpd) for AS2
- Admin (cmuadmind) for WebDAV

Use the following procedure to install the neccesary 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 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 Connect:Enterprise Remote Daemons on page 38*.
5. Refer to *Encrypting Internal Product Communications* on page 263 for information on encrypting communications between 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>deadmbox</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>deadmbox</DeadLetterMailbox>
      <SSLServer>
      </SSLServer>
   </Port>
</AS2Configuration>
```

5. To the SSLServer element, indicate the location of the key certificate you specified in step 1 on page 232 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>deadmbox</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>deadmbox</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>deadmbox</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 232 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 Connect:Enteprise UNIX server using the key certificate file.
- SERVERCLIENT = Client connections authenticate the Connect:Enterprise UNIX server using the Key certificate file. The Connect:Enterprise 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

Chapter 16

Configuring High Availability

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 Connect:Enterprise handles those failover capabilities.

Installing Connect:Enterprise High-Availability Scripts

The 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 Connect:Enterprise 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 Connect:Enterprise for the High-Availability Feature

If you decide to use the high availability feature after you install Connect:Enterprise, you must customize Connect:Enterprise manually using the following steps:

1. If you created a password for Connect:Enterprise and the system prompts for it at startup, add the CMUPASWD environment variable to the rcfiles kshrc, cshrc, and profile to enable 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 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 Connect:Enterprise user, change directories to $CMUHOME/etc, and run cehainstall.

   The following prompt is displayed:

```
The following directory (called the destination directory):
   /host/users/user01/ceunix21
was detected to be the location of Connect:Enterprise UNIX.

Is this correct? (Y|n)
```

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

```
================================================================================
=
Sterling Commerce, Inc., (TM) Connect:Enterprise UNIX (TM)
Version 1.3 High-Availability Package Installation Procedure

The Connect:Enterprise 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 Connect:Enterprise 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 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 Connect:Enterprise.

Connect:Enterprise Core High-Availability Scripts

This section describes the core scripts that 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 Connect:Enterprise UNIX in a high-availability environment.

Script	Description	Required Configuration
proc_mon.cfg	Used by all core scripts to start, stop, and monitor Connect:Enterprise processes and maintain a functioning system. It is the single point of process configuration for the Connect:Enterprise high-availability scripts.	A sample proc_mon_cfg is installed and configured by cehainstall. The cmuftpd protocol 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. To use the Site Administration user interface, add the cmusvid daemon (Service Interface daemon) and add the -p *portno* parameter, where *portno* specifies the port that the cmusvid daemon will monitor for inter-process communication. Refer to the *cmusvid—Service Interface Daemon* on page 110 for more information on the -p parameter.
ce_ha_start	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 ce_ha_start_cmuftpd starts cmuftpd by itself. This feature is used by ce_ha_probe to restart specific protocol daemons.	No configuration is necessary. **Note:** See the *Using Core Scripts without Implementing High Availability* on page 246 for information on using this script in an environment that does not implement the high-availability feature.
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.	No configuration is necessary. **Note:** See the *Using Core Scripts without Implementing High Availability* on page 246 for information on using the script in an environment that does not implement the high-availability feature.

Script	Description	Required Configuration
ce_ha_probe	Performs the following functions: ◆ Monitors the core daemons configured in the proc_mon.cfg file using the **ps** command. Upon failure of any of the core daemons, the probe script finishes active Connect:Enterprise processes and then fails over to the standby computer. ◆ Monitors any uncommented protocol daemons defined in the proc_mon.cfg file using the **ps** command. Upon failure of a protocol daemon, the probe script attempts to restart the daemon the number of times specified in proto.*retries* for that daemon. If the protocol cannot be restarted, the probe script stops Connect:Enterprise using ce_svc_stop, finishes active Connect:Enterprise processes, and fails over to the standby computer.	No configuration is necessary on the HP-UX platform. For AIX and Solaris platforms: 1. Open the $CMUHOME/etc/ha/ce_ha_probe file using vi or a similar text editor. The first portion of the file is marked as the user-modifiable section. 2. Edit the NOTIFY_FUNCTION 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.

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
process_name	Specifies the process name that returns when the **ps -edaf** command is issued. Indicates whether a given process is active or inactive.
process_owner	Specifies the process owner for the processes identified by the **ps -edaf** command. The default is the UNIX user who installed and runs Connect:Enterprise.

Value	Description
core|proto.*retries*	Determines what to restart in the event of a failover. core Sets value to core daemon. (cmuctld, cmuexitd, cmuacd, cmulogd, and cmumboxd). A core daemon failure results in Connect:Enterprise failing over. proto Sets 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*. **Note:** For bisync protocol on all platforms, set proto.r*etries* 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. **Note:** For FTP on the AIX platform, set proto.*retries* to proto.0 to initiate an immediate failover when the process started by the parent cmuftpd daemon is stopped and the Package Manager cannot restart the parent process because its child process continues running.
startup_command_line	Specifies the exact startup command needed to start the process. The ce_ha_start script has the 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 &
cmuftpd:uid1:proto.2:cmuftpd -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: 0 = All daemons are accounted for. 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 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 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 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 Connect:Enterprise, then start the ce_ha_probe script to monitor and restart 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 Connect:Enterprise, whereas the service monitor scripts start a monitor daemon that monitors the function of Connect:Enterprise. The monitor daemon restarts Connect:Enterprise if a failure occurs, and if the restart fails, it stops Connect:Enterprise and fails over to the standby host.

Note these important characteristics of the Sun implementation of high availability:

- 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 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 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 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 Connect:Enterprise. 0 = Start is successful. 1 = Start failed.
ce_svc_stop	Stops Connect:Enterprise cleanly. 0 = Stop is successful, or Connect:Enterprise was not running. Nonzero return = Stop failed. (The script was unable to stop Connect:Enterprise.) **Note:** If a shutdown cannot be done cleanly, the stop script forcibly stops all Connect:Enterprise processes as cleanly as possible.
ce_svc_probe	Polls the activity of 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 NCXDCMD 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 Connect:Enterprise with the Sun Package Manager

1. To register 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 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 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
/usr/cluster/bin/scswitch -R -h *hostname* -g ce-harg	Restarts the system.
/usr/cluster/bin/scswitch -z -g ce-harg -h *newhost*	Switches from one host to another specified by *newhost*.
/usr/cluster/bin/scswitch -c -h *hostname* -j ce-hars -f STOP_FAILED	Clears error flags. In this example, you received a STOP_FAILED when Connect:Enterprise could not cleanly shut down.
/usr/cluster/bin/scswitch -n -j ce-hars /usr/cluster/bin/scswitch -z -g ce-harg -h “” /usr/cluster/bin/scswitch -u -g ce-harg /usr/cluster/bin/scrgadm -r -j ce-hars /usr/cluster/bin/scrgadm -r -g ce-harg /usr/cluster/bin/scrgadm -r -t SCI.ce	Sequence of commands deletes resource and group definitions and unregisters Connect:Enterprise from the high-availability Package Manager configuration files. **Note:** The commands must be issued in the order they are listed here.
/usr/local/cluster/bin/scswitch -S -h *hostname* shutdown -g0 -y -i6	Reboots a cluster node cleanly.

Hewlett-Packard High-Availability Implementation

Connect:Enterprise UNIX is fully integrated with the Hewlett-Packard MC/ServiceGuard high-availability software. 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 Connect:Enterprise.

Note: MC/ServiceGuard does not use any of the core Connect:Enterprise high-availability scripts, but it does use the proc_mon.cfg configuration file. See the *Connect:Enterprise Core High-Availability Scripts* on page 243 and the *Syntax and Parameters for the proc_mon.cfg Script* on page 244 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 Connect:Enterprise. Initializes, terminates, starts, and stops the 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 Connect:Enterprise processes. It is called from control.sh.
ce_svc_stop	Stops Connect:Enterprise.

Configuration Files

Two configuration files are used with Connect:Enterprise. The package configuration file for 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 (Based on cluster; this parameter must be modified to reflect local settings.)
NODE_NAME	hp2 (Based on cluster; this parameter must be modified to reflect local settings.)
RUN_SCRIPT	/etc/cmcluster/ce/control.sh (Ensure that your scripts are located in /etc/cmcluster/ce.)
HALT_SCRIPT	/etc/cmcluster/ce/control.sh (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
SERVICE_HALT_TIMEOUT	300

Item	Value
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 (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 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 reformations.
# However, the use of the default value increases the potential
# for spurious reformations 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_TIMEOUT600000000
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 Connect:Enterprise for the HP High-Availability Environment

The following procedures outline the installation process and configuration changes required to use Connect:Enterprise in the Hewlett-Packard high-availability environment. Refer to the *Connect:Enterprise for UNIX Installation Guide* for complete, detailed instructions for installing 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 Connect:Enterprise as detailed in the *Connect:Enterprise UNIX Installation and Administration Guide*.
5. Set up and configure 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 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 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 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 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 Connect:Enterprise as detailed in the *Connect:Enterprise 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 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 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 *packagename*	Enables a package to fail over.
cmmodpkg -e *-n nodename packagename*	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 *packagename*	Halts the specified package.

Caution: In the event of a failure, all Connect:Enterprise processes being held are restarted when the ce package restarts, including any 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 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. 0 = Stop successful, or Connect:Enterprise is not running. Nonzero = Stop failed. (The script was unable to stop Connect:Enterprise.) **Note:** If a shutdown cannot be done cleanly, the stop script forcibly shuts down all Connect:Enterprise processes as cleanly as possible.
CE_probe.sh	Repeatedly polls the activity of 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 Connect:Enterprise can be restarted, the script returns a value of 0 (zero). Otherwise, it returns a value of nonzero.

Configuring the 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 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 Connect:Enterprise home directory available to all computers in the cluster.
3. Replace the value for NCXDPSSTRING (default of nxcd) 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 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 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 NXCDFILE 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 Connect:Enterprise with the AIX Package Manager

The following procedures illustrate how to register Connect:Enterprise with the AIX high-availability Package Manager, which allows the Package Manager to start, monitor, and stop Connect:Enterprise. If the service monitor stops, the AIX high-availability manager fails over to the standby computer.

Registering 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.

Chapter 17

Encrypting Internal Product Communications

Connect:Enterprise 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 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 Connect:Enterprise UNIX running, specify **Enable SIPS encryption=Yes** in the Define Configuration function of the Site Administration user interface.
2. Stop Connect:Enterprise UNIX. Refer to Chapter 5, *Starting and Stopping 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. Connect:Enterprise uses the encryption key to create session keys. A new session key is created each time Connect:Enterprise is started. 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 Connect:Enterprise UNIX. Refer to Chapter 5, *Starting and Stopping Connect:Enterprise* for more information.

Configuring for Connect:Enterprise Components Running on Different Computers

If you are running a Connect:Enterprise protocol daemon, API program, or offline command from a remote computer (any computer other than the computer Connect:Enterprise is running on), use the following procedure:

1. Place a copy of the sipskeys file generated in *Enabling Message Encryption* on page 263 in a directory on the computer that is running the 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 Connect:Enterprise Instances

If you are running a Connect:Enterprise GIS adapter, API program, or offline command on a remote computer (any computer other than the computer Connect:Enterprise is running on) that connects to multiple instances of Connect:Enterprise, use the following procedure:

1. Collect the sipskeys files for each instance of 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 Connect:Enterprise:

```
ceserver01 9976 o1FF9Bsp8pdBQSo+Aj6nUpvegA8d
ceserver02 9976 /S5HcclpNHpijdKnh1ipvFnzjBRo
ceserver03 9976 XsBb1hT3/IqH3DKQhLhTE82hlB/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
```

Appendix A

Error Messages

This chapter covers the following topics:

- Connect:Enterprise Error Codes
- Connect:Enterprise Error Codes–These errors are generated by the Command Line Utilities or by the 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).
- Connect:Enterprise API Error Codes–These errors are generated by the Command Line Utilities and user-written programs that use the Connect:Enterprise API. The utilities write these errors to stderr.
- Connect:Enterprise Auto Connect Status Codes–These status codes are displayed by the **cmureport** utility.
- Connect:Enterprise Remote Connect Status Codes–These status codes are displayed by the **cmureport** utility.
- Connect:Enterprise Utilities Exit Codes–These error codes are generated when Connect:Enterprise utilities exit.
- Authorization Log Message IDs–These error messages are displayed in the authentication log file.

Connect:Enterprise Error Codes

The following is the numerical listing of 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, Connect:Enterprise is automatically shutdown.	Determine what is causing the disk to be full and make adjustments. Ensure that the limits set for the 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_DECRYPTION_FAILED	Encrypted message received, but not decrypted.	Contact Sterling Commerce support.
526	0x020E	CMURC_SIPS_ENCRYPTION_FAILED	SIPS encryption failed.	Contact Sterling Commerce support.
527	0x020F	CMURC_SIPS_MSG_ENCRYPTED	Encrypted message was received, but a plain message was expected.	Contact Sterling Commerce support.
768	0x0300	CMURC_SIPS_MSG_NOT_ENCRYPTED	Plain message received, but encrypted message was expected.	Contact Sterling Commerce support.
769	0x0301	CMURC_SIPS_KEYFILE_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_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_INIT_ERROR	Cannot initialize SIPS encryption.	Contact Sterling Commerce support.
4096	0x1000	CMURC_SIP_BADSTATE	An unexpected message was received.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.
4097	0x1001	CMURC_HOST_NOT_FOUND	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 Connect:Enterprise operation.	Generate a level 99 debug trace and contact Sterling Commerce 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_ERRO R	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_ERR OR	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 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 Sterling Commerce Customer Service.
5121	0x1401	CMURC_SHARED_ATTACH_FAILED	Shared memory attach failed.	This error is posted when a 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 Sterling Commerce Customer Service.
5122	0x1402	CMURC_SHARED_DETACH_FAILED	Shared memory detach failed.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.
5123	0x1403	CMURC_SHARED_REMOVE_FAILED	Shared memory remove failed.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.
5376	0x1500	CMURC_SEM_CREATE_FAILED	Semaphore creation failed.	This error is posted when a 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 Sterling Commerce Customer Service.
5377	0x1501	CMURC_SEM_RM_FAILED	Semaphore removal failed.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.

Decimal	Hex	Error Text	Description	Action
5378	0x1502	CMURC_SEM_WAIT_FAILED	Semaphore wait failed.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.
5379	0x1503	CMURC_SEM_SIGNAL_FAILED	Semaphore signal failed.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.
5632	0x1600	CMURC_INVALID_FIELD_TYPE	Invalid field type passed to function.	Generate a level 99 debug trace and contact Sterling Commerce Customer Service.
5888	0x1700	CMURC_SESSION_ERROR	Error during session request. One or more daemons are hung.	Issue **cmushutdown** at earliest convenience and restart.
6143	0x17FF	CMURC_EACCESS	Access denied. The user is attempting an operation (like a **put** or **$$ADD**) that violates the security permissions defined in *$CMUHOME/med/mbxacl.conf*.	Update the mbxacl.conf 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 Sterling Commerce Customer Service.
6145	0x1801	CMURC_MBOXADD_FILE	I/O error opening file.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce Customer Service.
6146	0x1802	CMURC_MBOXADD_INDEXFILE	I/O error opening index file.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce Customer Service.
6147	0x1803	CMURC_MBOXADD_INDEXIO	I/O error writing index file.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce 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 Sterling Commerce Customer Service.

Decimal	Hex	Error Text	Description	Action
6149	0x1805	CMURC_MBOXADD_STATFS	I/O error getting file system information.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce Customer Service.
6150	0x1806	CMURC_MBOXADD_NOSPACE	Out of disk space.	Re-attempt failing operation after freeing some disk space.
6151	0x1807	CMURC_MBOXADD_SEEK	Seek error during add operation.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce 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 **cmuadd** command and retry.
6166	0x1816	CMURC_MBOXADD_LINK	Could not link to batch specified.	Verify existence of the file being referenced by the **cmuadd** command.
6167	0x1817	CMURC_MBOXADD_INDEXLINK	Could not link to index file for batch.	Generate a level 99 debug trace and contact Sterling Commerce 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 Sterling Commerce 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 Sterling Commerce Customer Service.

Decimal	Hex	Error Text	Description	Action
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 Sterling Commerce Customer Service.
6227	0x1853	CMURC_MBOXEXTRACT_INDEXIO	I/O error reading index file.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce Customer Service.
6228	0x1854	CMURC_MBOXEXTRACT_SEEK	Seek error while skipping control record.	Run file system consistency check (FSCK). If the problem continues, call Sterling Commerce Customer Service.
6229	0x1855	CMURC_SYS_RESOURCE_ERROR	Too many files open or too many Processes.	This error is posted when a 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 Sterling Commerce 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	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 **Security** and **Valid Mailbox ID list** parameters for **control.mcd**.
8193	0x2001	CMURC_SCRIPT_LOGIN_FAILED	Login from script failed.	Send/Expect portion of the login script failed. Verify the script.

Decimal	Hex	Error Text	Description	Action
8194	0x2002	CMURC_FAILED_TO_RECV_XLATEBUFFER	Failed to receive user translation buffer from control daemon.	Generate a level 99 debug trace and contact Sterling Commerce 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	Error during install while dialing.	Generate a level 4 debug trace of the Bisync daemon and contact Sterling Commerce Customer Service.
12290	0x3002	CMURC_BSC_ERROR_PORTSETUP	Error during port setup while dialing.	Generate a level 4 debug trace of the Bisync daemon and contact Sterling Commerce Customer Service.
12291	0x3003	CMURC_BSC_RT_NOTFOUND	Bisync runtime not found.	Verify the BSCRTDIR environment variable is set and is correct.
12292	0x3004	CMURC_BSC_RT_FAILED	Bisync runtime failed to start.	Call Sterling Commerce Customer Service.
12295	0x3007	CMURC_BSC_INTERRUPT	Process interrupted for AC. An idle leased line was interrupted to begin a Auto Connect.	No action necessary.
12296	0x3008	CMURC_BSC_GENERAL_ERROR	General error.	Generate a level 4 debug trace on the Bisync daemon and look for additional errors.
12297	0x3009	CMURC_BSC_RVI_RECEIVED	Reverse interrupt received from remote.	No action necessary
16384	0x4000	CMURC_JES_LOGON_FAILED	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_FAILED	JES2 logoff failed.	Check contents of logoff message for valid signon card against the LOGOFFMSG parameter in the RSD file for that remote.
20481	0x5001	CMURC_APS_M001E	Asset Protection - Item Key did not match - AP_Check()	Verify that the product was installed on the computer for which the asset protection keyfile was created.

Decimal	Hex	Error Text	Description	Action
20488	0x5008	CMURC_APS_M008E	Asset protection Key Validation failed - APKeyValid()	Check your asset protection keyfile for corruption or invalid information. If necessary, contact your Sterling Commerce account representative to request a new keyfile.
20496	0x5010	CMURC_APS_M010E	Asset Protection License has Expired (Warning)	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20497	0x5011	CMURC_APS_M011E	Asset Protection License is about to expire (Warning)	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20498	0x5012	CMURC_APS_M012E	Asset protection Initialization failed - AP_Init()	Verify that the asset protection keyfile is in the proper location and that there is sufficient memory available.
20499	0x5013	CMURC_APS_M013E	Asset Protection License has Expired (Halting)	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20500	0x5014	CMURC_APS_M014E	Asset Protection Option is not found	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20501	0x5015	CMURC_APS_M015E	Asset Protection Option has expired (Halting)	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20502	0x5016	CMURC_APS_M016E	Asset Protection Option has expired (Warning)	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20503	0x5017	CMURC_APS_M017E	Asset Protection Option is about to expire (Warning)	Contact your Sterling Commerce account representative to request a new asset protection keyfile.
20633	0x5099	CMURC_APS_M099E	Asset Protection Emergency Key has Expired	Contact your Sterling Commerce account representative to request a new asset protection keyfile.

Decimal	Hex	Error Text	Description	Action
28676	0x7004	CMURC_ SSH_CONNECTION_LOST	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_ 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 *Connect:Enterprise UNIX Remote User's Guide*.
28678	0x7006	CMURC_ SSH_FAILURE	General error.	View the trace file to identify the failure.
28679	0x7007	CMURC_ SSH_DIRECTORY	Path does not specify a regular file/batch. The specified path does not identify a file or a Connect:Enterprise UNIX batch.	Check the directory specified to ensured it identifies a file/batch.
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 Connect:Enterprise UNIX.

API Error Codes

The following is the numerical listing of the 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.

Decimal	Hex	Error Text	Description	Action
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_MSG	Unexpected message.	
16	0x0010	APIRC_GETHOST	gethostbyname failed.	
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.	

Decimal	Hex	Error Text	Description	Action
1281	0x0501	APIRC_GETDATA_FAILED	GetData callback failed.	
1537	0x0601	APIRC_ADDCARD_MISSING	**$$ADD** card missing in file.	
1538	0x0602	APIRC_ADDCARD_TO_LONG	**$$ADD** card to long.	
1539	0x0603	APIRC_ADDCARD_NO_RECSEP	**$$ADD** 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_WILDCARD	Wildcards in batch ID invalid.	
1544	0x0608	APIRC_BATCH_NO_INVALID	Batch number invalid.	
1792	0x0700	APIRC_SPLIT_TOO_SMALL	Splitcount parm too small.	
1793	0x0701	APIRC_NO_ACDLIST	AcdList not specified.	
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 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 GIS business process could not be started.	

Decimal	Hex	Error Text	Description	Action
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.	
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 Sterling Commerce 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.	

Decimal	Hex	Error Text	Description	Action
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 **cmucheckcfg** on the ACD and the RSD files for more specific information.
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 **cmucheckcfg** 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.	

Decimal	Hex	Error Text	Description	Action
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 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.

Decimal	Hex	Error Text	Description
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_SHAREDMEM	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 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 **cmuadd** is greater than 32 (**cmuadd** only).

Code	Description
8	No batches match selection criteria.
9	Out of disk space error (**cmuadd** only).
10.11.12	Connect:Enterprise general errors. For example, input file does not exist for cmuadd, Connect:Enterprise database error for cmuadd/cmuextract/cmustatus, batch data file not found for cmuextract.
13	System not up or invalid hostname or invalid port.
14	Could not create or open output file (**cmuextract** only).
15	Could not create or open report file (**cmuextract** only).
16	Could not create or open end data file (**cmuextract** 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."

Message ID	Qualifying Text	Message Short Text
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."
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."

Message ID	Qualifying Text	Message Short Text
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.

Message ID	Qualifying Text	Message Short Text
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.
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.

Message ID	Qualifying Text	Message Short Text
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.
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.

Message ID	Qualifying Text	Message Short Text
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”.

Message ID	Qualifying Text	Message Short Text
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 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, licensed=Y|N : <== External Authentication server settings	This message shows the configured settings for the External Authentication server. Connect=YES|NO indicates whether the authentication daemon is to establish a connection to the server. Start=YES|NO indicates whether the authentication daemon is to start the server. Licensed=YES|NO indicates whether external authentication support is licensed in $CMUHOME/etc/license.key. When not licensed, the server will not be started or connected to even if so configured.
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: 0x02 IDMBRC_INTERNAL_ERROR. Refer to *Additional Return Codes for AUTH0113* on page 290.
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 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.

Message ID	Qualifying Text	Description
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.
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.

Appendix B

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', 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 Connect:Enterprise to accommodate the new European monetary standard, the EURO.

```
0001020337402E2F1605250B0C0D0E0F
101112133C3D4B4B18193F271C1D1E1F
405A7F7B5B6C507D4D5D5C4E6B604B61
F0F1F2F3F4F5F6F7F8F97A5E4C7E6E6F
7CC1C2C3C4C5C6C7C8C9D1D2D3D4D5D6
D7D8D9E2E3E4E5E6E7E8E9ADE0BD5F6D
79818283848586878889919293949596
979899A2A3A4A5A6A7A8A9C06AD0A107
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B9F4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B4B
000102032E092E7F2E2E0A0B0C0D0E0F
10111213141516171819 1A1B1C1D1E1F
2E2E2E2E2E2E0A2E1B2E2E2E2E2E050607
2E2E2E2E2E2E2E2E2E2E2E2E2E14152E1A
202E2E2E2E2E2E2E2E2E2E2E3C282B2E
262E2E2E2E2E2E2E2E2E21242A293B5E
2D2F2E2E2E2E2E2E2E2E7C2C255F3E3F
2E2E2E2E2E2E2E2E2E603A2340273D22
2E6162636465666768692E2E2E2E2E2E
2E6A6B6C6D6E6F7071722E2E2E2E2EA4
2E7E737475767778797A2E2E2E5B2E2E
2E2E2E2E2E2E2E2E2E2E2E2E2E5D2E2E
7B41424344454647484 92E2E2E2E2E2E
7D4A4B4C4D4E4F5051522E2E2E2E2E2E
5C2E535455565758595A2E2E2E2E2E2E
30313233343536373839 2E2E2E2E2E2E
```

Glossary

Symbols

$$ADD

A command from a remote site signaling 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 Connect:Enterprise to delete a batch from the mailbox.

$$DIRECTORY

A command from a remote site requesting Connect:Enterprise for a partial or complete list of the mailbox contents.

$$REQUEST

A command from a remote site requesting Connect:Enterprise to send specified batches from the mailbox to its remote location.

A

account

Term used in the Connect:Enterprise UNIX Site Administration user interface to identify a file that defines a local user's password that allows access to local user commands on Connect:Enterprise UNIX, or a file that defines the communications and data characteristics of remote sites that are authorized to access Connect:Enterprise 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 (cmuadmind)

Daemon that communicates requests from the Connect:Enterprise Site Administration User Interface to the Service Interface Daemon (cmusvid). This enables Connect:Enterprise 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 Sterling Commerce API subroutines are responsible for performing inter-process communication with the appropriate 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 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 Connect:Enterprise 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 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 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 Connect:Enterprise UNIX Site Administration user interface provided with 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 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 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 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 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 be 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 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. 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 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 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 Gentran Integration Suite 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 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 Connect:Enterprise to begin the system shutdown procedure and end its processing.

ceustartup

A UNIX shell script to start the 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 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 Connect:Enterprise architecture is based on this paradigm.

cmuadd

A local-site command asking Connect:Enterprise to add specified batches to the mailbox.

cmuconnect

A local-site command asking Connect:Enterprise to activate the 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 Connect:Enterprise. This shell script is called by the **ceinstall** script.

cmudelete

A local-site command asking Connect:Enterprise to logically delete specified batches from the mailbox. Affected batches can be recovered by Connect:Enterprise with the **cmustatus** command after this operation.

cmuediintd

The EDIINT daemon used to package and unpackage AS2 messages.

cmuerase

A local-site command to Connect:Enterprise to physically erase specified batches from the mailbox. Erased batches cannot be recovered.

cmuextract

A local-site command to 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 Connect:Enterprise environment variable that defines the home or destination directory of all the Connect:Enterprise files.

CMUHOST

A Connect:Enterprise environment variable that defines the host name where the 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 Connect:Enterprise to list specified batches in the mailbox.

CMUPASWD

A 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 Connect:Enterprise utility.

CMUPORT

A Connect:Enterprise environment variable that defines the TCP/IP port number of the control daemon (*cmuctld*).

cmurefresh

A local-site command that instructs 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 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 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 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.*

Connect:Mailbox for MVS/VSE

A Sterling Commerce 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. Connect:Mailbox supports the standard protocols including SNA LU1, LU6.2, Bisync, Async and X.25, and provides open connections throughout CICS. Connect:Mailbox offers real-time, centralized management and control throughout the Connect:Mailbox network.

Connect:Enterprise

A Sterling Commerce 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. Connect:Enterprise UNIX supports the standard protocols including Bisync, Async, FTP, Secure FTP, HTTP, and Connect:Direct.

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 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. Connect:Enterprise is distributed as a cpio file.

cron

A UNIX command used to schedule routine and regular tasks such as file backup. In 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 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 Connect:Enterprise collects data from remote sites and stores it in the mailbox. Data collection means data is input from a remote site to Connect:Enterprise at the host computer.

data transmission

The process in which Connect:Enterprise transmits data from the Mailbox batch files to remote sites. Data transmission means data is output from 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 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 Connect:Enterprise.

del

The FTP command that, in 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 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 Connect:Enterprise, a formatted listing of control information for batches on 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 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 Connect:Enterprise 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 a Sterling Commerce 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 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 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 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 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 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 (cmuftpd)

The Communications daemon that manages all sessions established with remote sites through the FTP protocol.

function call

See *system call*.

G

GENTRAN

A Sterling Commerce EDI translation product.

get

The FTP command that, in 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 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 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 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. 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. 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 Connect:Enterprise. Local users are directly connected to this host computer and directly execute Connect:Enterprise programs.

log

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

Log Daemon (cmulogd)

The 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 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 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 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 Connect:Enterprise, the area where batches are stored.

Mailbox Control Definitions File (MCD)

The file containing the 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 Connect:Enterprise.

Mailbox Daemon (cmumboxd)

The 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 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. 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 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 reconverting 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 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 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 Connect:Enterprise, the state that allows remote sites to access batches in the mailbox. 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, 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 Connect:Enterprise, the communications protocols are Async, Bisync, FTP, HTTP.

put

The FTP command that, in 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 indicated that the 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 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 Connect:Enterprise 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 Connect:Enterprise UNIX Site Administration user interface to describe the 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 Connect:Enterprise 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 Connect:Enterprise UNIX Site Administration user interface and the Connect:Enterprise UNIX server.

session

A logical connection between Connect:Enterprise at the local site and another computer at the remote site. When a logon command is completed between 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 Connect:Enterprise session that is checked into control subsystem (*cmuctld*). A session is defined as any Connect:Enterprise subsystem (*cmuexitd*, *cmuasyd*, *cmuftpd, cmumboxd* and so on) or any of a remote connects serviced by a copy of the communication subsystems (*cmuftpd*, *cmuasyd, cmubscda, cmubscdc*), command line utilities (**cmuadd, cmuextract,** and so on). All of these instances has to check in with 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 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 Sterling Commerce'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. Connect:Enterprise 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.

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 Connect:Enterprise, the ability to create a snapshot of a dump of internal 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. 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 $TURNLINE$ 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 $TURNLINE$.

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 Connect:Enterprise at appropriate times during the processing of a transaction. The user-supplied program can alter the standard processing done by 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 Connect:Enterprise commands as well as to automate the system.

userid

In 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.

Index

A

B

C

D

E

F

G

H

I

J

L

M

O

P

Q

R

S

T

U

V

W

As set forth below, certain of the Third Party Licensors assert the following terms with respect to their respective products. Such terms shall only apply as to the specific Third Party Licensor product and not to those portions of the product derived from other Third Party Licensor products or to the Sterling Commerce Software product as a whole.

Those portions of the Sterling Commerce Software which include, or are distributed on the same storage media with, the Third Party Software where use, duplication, or disclosure by the United States government or a government contractor or subcontractor, are provided with RESTRICTED RIGHTS under Title 48 CFR 2.101, 12.212, 52.227-19, 227.7201 through 227.7202-4, FAR 52.227-14 and FAR 52.227-19(c)(1-2) and (6/87), and where applicable, the customary Sterling Commerce license, as described in Title 48 CFR 227-7202 with respect to commercial software and commercial software documentation including DFAR 252.227-7013, DFAR 252.227-7014, DFAR 252.227-7015 and DFAR 252.227-7018, all as applicable.

The Sterling Commerce Software and the related documentation are licensed either "AS IS" or with a limited warranty, as set forth in the Sterling Commerce license agreement. Other than any limited warranties provided, NO OTHER WARRANTY IS EXPRESSED AND NONE SHALL BE IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR USE OR FOR A PARTICULAR PURPOSE. The applicable Sterling Commerce entity reserves the right to revise this publication from time to time and to make changes in the content hereof without the obligation to notify any person or entity of such revisions or changes.

Except as otherwise set forth below, the Third Party Software is provided 'AS IS' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. FURTHER, IF YOU ARE LOCATED OR ACCESSING THIS SOFTWARE IN THE UNITED STATES, ANY EXPRESS OR IMPLIED WARRANTY REGARDING TITLE OR NON-INFRINGEMENT ARE DISCLAIMED.

XALAN-J AND XERCES-J

The Sterling Commerce Software is distributed with or on the same storage media as the Xalan-J and Xerces-J software (together, the "Xalan and Xerxes Software") located at $CMUHOME/javalib/xalan.jar, xerxesImpl-2_1_1.jar, and xmlParserAPIs-2_1_1.jar. Use of the Xalan and Xerxes Software is subject to the terms of the following license:

The Apache Software License, Version 1.1

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software
Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Xalan", "Xerces" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JETTY SOFTWARE
The Sterling Commerce Software is distributed with or on the same storage media as the Jetty Software, located at $CMUHOME/jetty-4.2.21-jdk1.2.jar, which is subject to the following license:

From http://jetty.mortbay.org/jetty/LICENSE.html:

Jetty License
$Revision: 3.7$

Preamble:
The intent of this document is to state the conditions under which the Jetty Package may be copied, such that the Copyright Holder maintains some semblance of control over the development of the package, while giving the users of the package the right to use,

distribute and make reasonable modifications to the Package in accordance with the goals and ideals of the Open Source concept as described at http://www.opensource.org.

It is the intent of this license to allow commercial usage of the Jetty Package, so long as the source code is distributed or suitable visible credit given or other arrangements made with the copyright holders.

Definitions:

- "Jetty" refers to the collection of Java classes that are distributed as a HTTP server with servlet capabilities and associated utilities.
- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.
- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.
- "Copyright Holder" is whoever is named in the copyright or copyrights for the package. Mort Bay Consulting Pty. Ltd. (Australia) is the "Copyright Holder" for the Jetty Package.
- "You" is you, if you're thinking about copying or distributing this Package.
- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)
- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

0. The Jetty Package is Copyright © Mort Bay Consulting Pty. Ltd. (Australia) and others. Individual files in this Package may contain additional copyright notices. The javax.serviet packages are copyright
Sun Microsystems Inc.
1. The Standard Version of the Jetty package is available from
http://jetty.mortbay.org.
2. You may make and distribute verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you include this license and all of the original copyright notices
and associated disclaimers.
3. You may make and distribute verbatim copies of the compiled form of the Standard Version of this Package without restriction, provided that you include this license.
4. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.
5. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do
at least ONE of the following:

a) Place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
b) Use the modified Package only within your corporation or organization.
c) Rename any non-standard classes so the names do not conflict with standard classes, which must also be provided, and provide a separate manual page for each non-standard class that clearly documents how it differs from the Standard Version.
d) Make other arrangements with the Copyright Holder.
6. You may distribute modifications or subsets of this Package in source code or compiled form, provided that you do at least ONE of the following:
a) Distribute this license and all original copyright messages, together with instructions (in the about dialog, manual page or equivalent) on where to get the complete Standard Version.
b) Accompany the distribution with the machine-readable source of the Package with your modifications. The modified Package must include this license and all of the original copyright notices and associated disclaimers, together with instructions on where to get the complete Standard Version.
c) Make other arrangements with the Copyright Holder.
7. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you meet the other distribution requirements of this license.
8. Input to or the output produced from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially,
and may be aggregated with this Package.
9. Any program subroutines supplied by you and linked into this Package shall not be considered part of this Package.
10. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
11. This license may change with each release of a Standard Version of the Package. You may choose to use the license associated with version you are using or the license of the latest Standard Version.
12. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
13. If any superior law implies a warranty, the sole remedy under such shall be, at the Copyright Holders option either a) return of any price paid or b) use or reasonable endeavors to repair or replace the software.
14. This license shall be read under the laws of Australia.
The End

This license was derived from the Artistic license published on
http://www.opensource.com

OPEN SSL SOFTWARE
The Sterling Commerce Software is distributed with or on the same storage media as the OpenSSL Software, located at$CMUHOME/<os>/bin/*ftp*. The OpenSSL Software is distributed under a dual license, as set out below:

OpenSSL License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in
the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young
(eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF

THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

OPENSSH SOFTWARE

The Sterling Commerce Software is distributed with or on the same storage media as the OpenSSH Software, located at $CMUHOME/<os>/bin/*ssh*. Copyright © 1995 Tatu Ylonen <ylo@cs.hut.fi>. Any information and cryptographic algorithms used in the OpenSSH Software are publicly available on the Internet and more information can be found at http://www.cs.hut.fi/crypto.

ANTLR

The Sterling Commerce software is distributed with or on the same storage media as the Antlr software, located at $CMUHOME/javalib/antlr.jar, which is subject to the following license:

[The BSD License]
Copyright (c) 2005, Terence Parr
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

COMMONS CODE C, FOP, COMMONS BEANUTILS PACKAGE, COMMONS LOGGING PACKAGE, HIVEMIND, TEXT ORO, XALAN-JAVA, AVALON, BATIK, CATALINA, TOMCAT, NAMING-RESOURCES,, LOG4J AND HTTP CLIENT.
The Sterling Commerce Software is distributed with or on the same storage media as the following software products: Commons Code C, FOP, Commons Beanutils Package, Commons Logging Package, Hivemind, Text ORO, Xalan-Java, Avalon, Batik, Catalina, Tomcat, Naming-Resources, log4j, and HTTP Client, (collectively, "Apache 2.0 Software").

Sterling Commerce has made no modifications to Apache 2.0 Software files.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes

of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally

submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent

to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

UTIL.CONCURRENT

The Sterling Commerce Software is distributed with or on the same storage media as the Util.Concurrent Software, located at $CMUHOME/javalib/concurrent1.3.2.jar which is subject to the following license:

All classes of util.concurrent release 1.3.4 were released to the public domain and may be used for any purpose whatsoever without permission or acknowledgment. [http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html].

Portions of the CopyOnWriteArrayList and ConcurrentReaderHashMap classes are adapted from Sun JDK source code. These are copyright of Sun Microsystems, Inc, and are used with their kind permission, as described in this license:

TECHNOLOGY LICENSE FROM SUN MICROSYSTEMS, INC.
TO DOUG LEA

Whereas Doug Lea desires to utilized certain Java Software technologies in the util.concurrent technology; and
Whereas Sun Microsystems, Inc. (“Sun”) desires that Doug Lea utilize certain Java Software technologies in the util.concurrent technology;

Therefore the parties agree as follows, effective May 31, 2002:
“Java Software technologies” means classes/java/util/ArrayList.java, and classes/java/util/HashMap.java.

Sun hereby grants Doug Lea a non-exclusive, worldwide, non-transferrable license to use, reproduce, create derivate works of, and distribute the Java Software and derivative works thereof in source and binary forms as part of a larger work, and to sublicense the right to use, reproduce and distribute the Java Software and Doug Lea's derivative works as the part of larger works through multiple tiers of sublicensees provided that the following conditions are met:

-Neither the name of or trademarks of Sun may be used to endorse or promote products including or derived from the Java Software technology without specific prior written permission; and

-Redistributions of source or binary code must contain the above copyright notice, this notice and the following disclaimers:
This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN MICROSYSTEMS, INC. OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
You acknowledge that Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

signed [Doug Lea]

dated

JAXB SOFTWARE

The Sterling Commerce Software is distributed with or on the same storage media as the JAXB Software, located at $CMUHOME/javalib/jaxb-api.jar, jaxb-libs.jar, jaxb-ri.jar, and jaxb-api.jar, which is subject to the following license:

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0 (text)

* 1. Definitions.

o 1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.

o 1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

o 1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

o 1.4. Executable means the Covered Software in any form other than Source Code.

o 1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.

o 1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

o 1.7. License means this document.

o 1.8. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

o 1.9. Modifications means the Source Code and Executable form of any of the following:

* A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;

* B. Any new file that contains any part of the Original Software or previous Modification; or

* C. Any new file that is contributed or otherwise made available under the terms of this License.

o 1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.

o 1.11. Patent Claims means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

o 1.12. Source Code means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.

o 1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, You includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

* 2. License Grants.
o 2.1. The Initial Developer Grant.
Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:
* (a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and
* (b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).
* (c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.
* (d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.
o 2.2. Contributor Grant.
Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:
* (a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and
* (b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).
* (c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.
* (d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.
* 3. Distribution Obligations.
o 3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License. You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

o 3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

o 3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

o 3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

o 3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

o 3.6. Larger Works.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

* 4. Versions of the License.

o 4.1. New Versions.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

o 4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

o 4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

* 5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN AS IS BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

* 6. TERMINATION.

o 6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

o 6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as Participant) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice

from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

o 6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

* 7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTYS NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

* 8. U.S. GOVERNMENT END USERS.

The Covered Software is a commercial item, as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of commercial computer software (as that term is defined at 48 C.F.R. 252.227-7014(a)(1)) and commercial computer software documentation as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

* 9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdictions conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree

that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.
* 10. RESPONSIBILITY FOR CLAIMS.
As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.
ZLIB SOFTWARE

The Sterling Commerce Software is distributed with or on the same storage media as the Zlib Software, located at $CMUHOME/<os>/bin/*ftp* and *ssh* which is subject to the following license:

zlib License
License
/* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org
Mark Adler madler@alumni.caltech.edu

LIBXML and LIBXSLT SOFTWARE:

The Sterling Commerce software is distributed with or on the same storage media as the LibXML software, and the LibXSLT Software, located at $CMUHOME/<os>/bin/cmusvwd, which are both subject to the following license:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JDOM
The Sterling Commerce Software is distributed with or on the same storage media as the JDOM Software, located at $CMUHOME/javalib/jdom.jar, which is subject to the following license:

LICENSE

Copyright (C) 2000-2004 Jason Hunter & Brett McLaughlin. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <request_AT_jdom_DOT_org>.

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management <request_AT_jdom_DOT_org>.

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter <jhunter_AT_jdom_DOT_org> and Brett McLaughlin <brett_AT_jdom_DOT_org>. For more information on the JDOM Project, please see <http://www.jdom.org/>.