



Installing Cisco EPOM

This chapter contains the following topics:

- [About Cisco EPOM Installation, page 2-1](#)
- [Upgrading Cisco EPOM, page 2-4](#)
- [Configuring EPOM Authentication Using a Separate RADIUS Server, page 2-5](#)
- [Configuring SSL Corba for Secure Communication Between Cisco EPOM and Cisco BTS 10200, page 2-6](#)
- [Starting Cisco EPOM, page 2-7](#)
- [Stopping Cisco EPOM, page 2-7](#)
- [Reinitializing the MySQL and Cisco EPOM Databases, page 2-8](#)
- [Accessing Cisco EPOM, page 2-8](#)
- [Logging Into Cisco EPOM, page 2-9](#)

About Cisco EPOM Installation

Cisco EPOM installation sets up two separate directories:



Note

The installation information in this section shows that Cisco EPOM is installed in the `/opt/CSCOepom` directory.

- Application directory is `/opt/CSCOepom` directory
Do not create or modify any of the files in this directory.
- Data directory is `var/opt/CSCOepom` directory
This is the location of log files and live data.



Note

This directory is not deleted when you uninstall the Cisco EPOM application.

During its initial installation, Cisco EPOM creates and initializes a database that is used to store user IDs, login passwords, group information, and device inventories.

During installation, if an existing database is detected, the installation script does not reinitialize the database. You can determine if the database must be reinitialized, but this is not recommended.

To reinitialize the database, see the [“Reinitializing the MySQL and Cisco EPOM Databases”](#) section on page 2-8.

Prerequisites for Installing Cisco EPOM

Before you install Cisco EPOM, check that the Cisco BTSdis package is installed on both the Cisco BTS 10200 EMS primary and secondary servers. See the *Cisco BTS 10200 Softswitch Application Installation*.

You can also check if the CORBA application is running on the Cisco BTS 10200 EMS servers as described in the *Cisco BTS 10200 Softswitch Application Installation*.

If you intend to use a RADIUS server for Cisco EPOM authentication, verify that RADIUS server is running and all logins, shared secret keys, Cisco EPOM server IP address / hostname and other relevant information is configured on the RADIUS server.

See the [“Configuring EPOM Authentication Using a Separate RADIUS Server”](#) section on page 2-5

Cisco EPOM server is shipped along with relevant SSL keystore, truststore and certificate.

Before you install EPOM, check if the following operating system packages are installed.

SUNWxwacx	AccessX client program
SUNWxwcft	X Window System common (not required) fonts
SUNWxwctl	X Window System Display Postscript CID support library
SUNWxwdv	X Windows System Window Drivers
SUNWxwdvx	X Windows System Window Drivers (64-bit)
SUNWxwft	X Window System platform required fonts
SUNWxwfs	Font server
SUNWxwhl	X Window System & Graphics Header links in /usr/include
SUNWxwice	ICE components
SUNWxwicx	X Window System ICE library (64-bit)
SUNWxwinc	X Window System include files
SUNWxwkey	X Windows software, PC keytables
SUNWxwman	X Window System online user man pages
SUNWxwmod	OpenWindows kernel modules
SUNWxwmox	X Window System kernel modules (64-bit)
SUNWxwoft	X Window System optional fonts
SUNWxwopt	nonessential MIT core clients and server extensions
SUNWxwplt	X Window System platform software
SUNWxwplx	X Window System library software (64-bit)
SUNWxwpmn	X Window System online programmers man pages
SUNWxwpsr	Sun4u-platform specific X server auxiliary filter modules

SUNWxwrtl	X Window System & Graphics Runtime Library Links in /usr/lib
SUNWxwrtx	X Window System Runtime Compatibility Package (64-bit)
SUNWxwslb	X Window System static/lint libraries
SUNWxwslx	X Window System lint libraries (64-bit)
SUNWxwsrc	X Window System sample source

To check if these packages are installed, execute the following commands:

- `cd /var/sadm/pkg`
- `pkginfo SUNWxw*`


Note

EPOM cannot be installed along with BTS EMS. The Solaris jumpstart image for BTS EMS does not contain all the required packages for EPOM installation.

Installing Cisco EPOM

You can install Cisco EPOM on a server that meets Cisco EPOM platform requirements.

-
- Step 1** Change the user to superuser by entering:
- ```
su - root
```
- Step 2** Download the Cisco EPOM image from this location:
- <http://www.cisco.com/cgi-bin/tablebuild.pl/epom45>
- Step 3** Extract the tarfile:
- ```
tar -xvf epom-n_n_n_x-nnnnnnnn-n.tar
```
- Step 4** Change the working directory by entering:
- ```
cd epom-n_n_n_x-nnnnnnnn-n
```
- Step 5** Run the Setup script:
- ```
./setup
```
- Step 6** Remove the installation image by entering these commands:
- ```
cd epom-n_n_n_x-nnnnnnnn-n
rm -f epom-n_n_n_x-nnnnnnnn-tar
rm -rf epom-n_n_n_x-nnnnnnnn-n
```
- The working Cisco EPOM image is installed in the `/opt/CSCOepom` directory.
- 

## Uninstalling Cisco EPOM

After you uninstall Cisco EPOM, you must manually delete the data files from the `/var/opt/CSCOepom` directory. These files are not automatically deleted by the uninstallation process.

- 
- Step 1** Change the user to superuser by entering:
- ```
su - root
```
- Step 2** Check that you are not in the /opt/CSCOepom directory.
- Step 3** Run the uninstallation script by entering:
- ```
/opt/CSCOepom/uninstall/uninstall
```
- 

## Upgrading Cisco EPOM

This procedure shows you how to upgrade from Cisco EPOM Release 1.5 to Cisco EPOM Release 4.5. Follow the same procedure in order to upgrade to Cisco EPOM Release 4.5 from any other previous version of EPOM

- 
- Step 1** Change the user to superuser by entering:
- ```
su - root
```
- Step 2** Create a temporary directory (epom_install2) for the Cisco EPOM 4.5 image:
- ```
cp epom-4_5_20041216-1.tar /opt/epom_install2
cd /opt/epom_install2
```
- Step 3** Extract the image from the tarfile:
- ```
tar -xvf epom-4_5_20041216-1.tar
```
- Step 4** List the image contents:
- ```
ls
epom-4_5_20041216-1 epom-4_5_20041216-1.tar
```
- Step 5** Change to the location of the new, untarred image:
- ```
cd epom-4_5_20041216-1
```
- Step 6** Start installing the new image:
- ```
./setup
```
- This message appears:
- ```
Warning:
The Extensible Provisioning and Operations Manager 1.5 (3) is currently installed and must
be uninstalled before this version is installed.
```
- Step 7** Confirm that you want to uninstall your current version of Cisco EPOM. To do this select **y** at this prompt:
- ```
Do you wish to uninstall this product [y,n,?]
```

A message appears:

Note: The CSCOpom data directory, /var/opt/CSCOpom still exists and must be removed manually.

```
Using previously installed MySQL database.
```

```
Using previously installed EPOM database.
```

```
Verifying EPOM Database.
```

```
Starting mysqld daemon with databases from /var//opt/CSCOpom/data/db
```

```
MySQL Server has started
```

```
Verifying EPOM Database Tables
```

```
Extensible Provisioning and Operations Manager installation is complete.
```

To reinitialize the Cisco EPOM database, see the [“Reinitializing the MySQL and Cisco EPOM Databases” section on page 2-8](#).

---

## Configuring EPOM Authentication Using a Separate RADIUS Server

The external RADIUS IETF Server usage is optional. If EPOM requires a radius authentication, then the external Radius IETF Server must be running and configured in order to be used by Cisco EPOM Server.

See the [“Prerequisites for Installing Cisco EPOM” section on page 2-2](#)

---

**Step 1** Log into EPOM web server via telnet or ssh session with root login, type:

```
cd /opt/CSCOpom/tomcat/webapps/ROOT/WEB-INF/classes/com/cisco/opus/
props
```

**Step 2** Edit the following parameters in main.properties file, as suitable to your setup environment:

```
radius.enable=no
radius.ip=10.76.62.105
radius.sharedsecret=1001
radius.authenticationPort=1812
radius.accountingPort=1813
```

By default the Radius Enable flag is set to **no**. It means that Radius server will not be used for EPOM authentication. If EPOM requires Radius authentication, then update the Radius enable flag to **yes**.

In this case 10.76.62.105 is the IP address of our RADIUS server, 1001 is the shared secret key for the IP address / hostname of the Cisco EPOM server and the RADIUS server's authenticationPort, accountingPort are 1812, 1813 respectively.

Generally you do not need to change the authenticationPort, accountingPort, unless you have modified these on your RADIUS server.

---

# Configuring SSL Corba for Secure Communication Between Cisco EPOM and Cisco BTS 10200

Cisco EPOM server is shipped along with relevant SSL keystore, truststore and certificate. This section should only be referred to, in case you change the default Cisco EPOM installation directory from `/opt/CSCOepom` to some other directory.

The default SSL configuration can be viewed as follows:

---

**Step 1** Log into EPOM web server via telnet or ssh session with root login, type:

```
cd /opt/CSCOepom/tomcat/webapps/ROOT/WEB-INF/classes/com/cisco/opus/
props
```

**Step 2** View the following parameter in main.properties file:

```
corba.orb.configfile=/opt/CSCOepom/tomcat/ssliiop/OpenORB.xml
```

**Step 3** List the SSL files:

```
cd /opt/CSCOepom/tomcat/ssliiop
```

The following files appear:

```
ls
bts10200.cer bts10200_ts OpenORB.xml pss.xml
bts10200_ks default.xml ots.xml SSLIOP.xml
```

**Step 4** View the following parameters in the SSLIOP.xml file:

```
<property name="context.keyStore.URL" value = "/opt/CSCOepom/tomcat/ssliiop/bts10200_ks"
/>

<property name="context.trustStore.URL" value = "/opt/CSCOepom/tomcat/ssliiop/bts10200_ts"
/>
```

---

In case you install Cisco EPOM under directory `/opt/myEPOM`, then following changes need to be made in order to configure Corba over SSL:

---

**Step 1** Log into EPOM web server through Telnet or ssh session with root login, type:

```
cd /opt/myEPOM/tomcat/webapps/ROOT/WEB-INF/classes/com/cisco/opus/
props
```

**Step 2** Change the corba.orb.configfile value in main.properties file as follows:

```
corba.orb.configfile=/opt/myEPOM/tomcat/ssliiop/OpenORB.xml
```

**Step 3** List the SSL files:

```
cd /opt/myEPOM/tomcat/ssliiop
```

The following files appear:

```
ls
bts10200.cer bts10200_ts OpenORB.xml pss.xml
bts10200_ks default.xml ots.xml SSLIOP.xml
```

**Step 4** Change the value of following parameters in the SSLIOP.xml file:

```
<property name="context.keyStore.URL" value = "/opt/myEPOM/tomcat/ssliiop/bts10200_ks" />
```

```
<property name="context.trustStore.URL" value = "/opt/myEPOM/tomcat/ssliiop/bts10200_ts" />
```

---

## Starting Cisco EPOM

The Cisco EPOM web server must be running in order to be accessed by web clients.

**Step 1** From the EPOM web server, type:

```
/opt/CSCOepom/bin/epom start
```

You will see the following:

```
% /opt/CSCOepom/bin/epom start
```

```

Starting EPOM

```

**Step 2** Enter responses to the InstallShield Wizard sequence.

When the installation is complete, the following message appears:

```
Starting MySQL
MySQL server is already started
Starting Tomcat
Tomcat has started

```

```
EPOM Started

```

---

## Stopping Cisco EPOM

To stop Cisco EPOM, do the following:

From the EPOM web server, type:

```
/opt/CSCOepom/bin/epom stop
```

The following message appears:

```
% /opt/CSCOepom/bin/epom stop
```

```

Stopping EPOM

```

```
Stopping MySQL
041216 15:26:12 mysqld ended (This appears only in the window from which EPOM was started)
MySQL server has stopped
Stopping Tomcat
Tomcat has stopped

```

```
EPOM Stopped

```

---

## Reinitializing the MySQL and Cisco EPOM Databases

You can reinitialize the MySQL and Cisco EPOM databases for these reasons:

- To reset the Admin password necessary to log in to Cisco EPOM.
- To clear the databases following a Cisco EPOM upgrade.

Reinitialize the MySQL and Cisco EPOM databases by entering:

```
/opt/CSCOepom/mysql/install/bin/installMySQLDB -ifs
/opt/CSCOepom/mysql/install/bin/installEPOMDB -ifs
```

If you reinitialize the MySQL database, you must initialize the Cisco EPOM database as well.

## Accessing Cisco EPOM

You can access Cisco EPOM from a web browser. (For supported web browsers, see the [“Cisco EPOM Client Requirements” section on page 1-3.](#))

Before you start Cisco EPOM, you will need this information:

- Tomcat non-secure port number
- Tomcat secure port number

You can also select the defaults displayed for these ports.

For a Secure connection:

- If you are using the default port 443, enter:

```
https://EPOMhostname
```

- If you are using any other port, enter:

```
https://EPOMhostname:port number
```

Where

*EPOMhostname*—The host machine where Cisco EPOM is installed.

*port number*—Identifies the port that is used.

For an Insecure connection:

- If you are using port 80, enter:

```
http://EPOMhostname
```

- If you are using any other port (default installed port is 8080), enter:

```
http://EPOMhostname:port number
```

Where

*EPOMhostname*—The host machine where Cisco EPOM is installed.

*port number*—Identifies the port that is used.

# Logging Into Cisco EPOM

To log into Cisco EPOM, do the following:

- 
- Step 1** Launch a web browser. (For supported web browsers, see the [“Cisco EPOM Client Requirements” section on page 1-3.](#))
  - Step 2** Access Cisco EPOM (see the [“Accessing Cisco EPOM” section on page 2-8.](#))
  - Step 3** Log in with the default admin account:  
User Name: `admin`  
Password: `admin`
  - Step 4** Click **Login**.  
You can now build a Cisco EPOM inventory as described in [Chapter 3, “Setting Up Cisco EPOM.”](#)
-

