CHAPTER 5

Configuring SSL Between Gateways and Units

The following topics tell you how to configure SSL between gateways and units:

- Enabling SSL on Gateways and Units, page 5-1
- Viewing and Exporting SSL Certificates, page 5-4
- Viewing SSL Status and Print SSL Certificates, page 5-4
- Disabling SSL, page 5-5

Enabling SSL on Gateways and Units

To enable user access (see Setting User Access, page 6-1), SSL must be enabled on Prime Performance Manager gateways and units. This process includes the generating the SSL key and certificate for the gateway and each unit connected to it, and then importing the corresponding SSL key and certificate to the gateway and units. Units must have the SSL certificate of the gateway to which it is assigned; the gateway must have the SSL certificate for each unit connected to it.

Enabling SSL on gateways and units is performed using the ppm ssl enable command. For the gateway and collocated unit, the SSL key and certificate generation and respective certificate imports are performed automatically. If you have remote units, you must copy the gateway SSL certificate to the unit and perform a number of steps manually.

Note Enabling SSL requires the gateway and unit(s) to be stopped and restarted.

To enable SSL, complete one or both of the following procedures:

- Enabling SSL on a Gateway or Collocated Gateway and Unit, page 5-1
- Enabling SSL on Remote Units, page 5-3

Enabling SSL on a Gateway or Collocated Gateway and Unit

To enable SSL on the Prime Performance Manager gateway or collocated gateway and unit:

Step 1 Log into the gateway as the root user.

Step 2 Enter the ssl enable command:

```
/opt/CSCOppm-gw/bin/ppm ssl enable
```

Prime Performance Manager:

- Stops the gateway.
- Stops the collocated unit.
- Generates RSA private key.

Step 3 When prompted, enter the SSL distinguishing information for the gateway:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager:

- Generates the following files on the gateway /opt/CSCOppm-gw/etc/ssl directory:
  - server.key—The gateway private key. Keep this key protected from unauthorized personnel.
  - server.crt—The self-signed SSL certificate.
  - server.csr—The certificate signing request (CSR). (The CSR is not used if you are using a self-signed SSL certificate.)
- Imports the gateway SSL certificate to the collocated unit.

Step 4 When prompted, enter the SSL distinguishing information for the collocated unit:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager:

- Generates the server.key, server.crt, and server.csr on the unit /opt/CSCOppm-unit/etc/ssl directory.
- Imports the collocated unit SSL certificate to the gateway.

Step 5 You are prompted to restart the gateway and unit:

```
Restart gateway and unit now (y/n)?
```

Enter **y** if you want to restart the gateway and collocated unit now, or **n** if you want to restart them later.

Note If you will enable SSL on remote units, choose **n** and continue with the "Enabling SSL on Remote Units" procedure on page 5-3. You will restart the gateway after you enable SSL on the remote units.

Note You can restart the gateway and collocated unit at any later time using the command: **/opt/CSCOppm-gw/bin/ppm restart**

Enabling SSL on Remote Units

To enable SSL on remote units:

Step 1 Log in to the remote unit.

Step 2 Enable SSL on the unit:

```
/opt/CSCOppm-unit/bin/ppm ssl enable
```

Prime Performance Manager:

- Stops the unit.
- Generates RSA private key.

Step 3 When prompted, enter the SSL distinguishing information for the unit:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager generates the server.key, server.crt, and server.csr on the unit /opt/CSCOppm-unit/etc/ssl directory:

Step 4 Import the unit certificate to the gateway:

a. Copy the **/opt/CSCOppm-unit/etc/ssl/server.crt** to a temporary location on the gateway, for example, /tmp/server.crt.

b. Enter the following command to import the unit certificate:

```
/opt/CSCOppm-gw/bin/ppm certtool import myhostname-unit -file filename
```

Where *alias* is a string alias for the certificate file and *filename* is the full path name for the certificate file, for example, /tmp/server.crt. Each imported certificate must have a unique alias when imported.

Step 5 Import the gateway certificate to the unit:

a. Copy the **/opt/CSCOppm-gw/etc/ssl/server.crt** to a temporary location on the unit machine, for example, /tmp/server.crt.

b. Import the gateway certificate:

```
/opt/CSCOppm-unit/bin/ppm certtool import myhostname-gateway -file filename
```

Where *alias* is a string that is an alias for the certificate file and *filename* is the full path name for the certificate file, for example, /tmp/server.crt.

Note The gateway imports the certificate file for each unit that connects to it. Each unit then imports the gateway certificate file for the gateway that it connects to.

Step 6 Restart the gateway:

```
/opt/CSCOppm-gw/bin/ppm restart
```

Step 7 Restart the remote unit:

```
/opt/CSCOppm-unit/bin/ppm restart unit
```

Step 8 If you previously established the Cisco Prime Network cross-launch, complete the Enabling Prime Performance Manager Cross-Launches from Prime Network, page 4-3 procedure to ensure the cross-launch links to are updated.

Related Topics:

Viewing and Exporting SSL Certificates, page 5-4

Viewing SSL Status and Print SSL Certificates, page 5-4

Disabling SSL, page 5-5

Viewing and Exporting SSL Certificates

If you implemented SSL in Prime Performance Manager, you can export SSL certificates that have been imported to Prime Performance Manager gateways or units.

To export a SSL certificate, enter the following command:

/opt/CSCOppm-gw/bin/ppm certtool export *alias* **-file** *filename*

where *alias* is the alias used when the certificate was imported and *filename* is the output file for the certificate.

To view detailed information about an SSL certificate, click the locked padlock icon in the lower-left corner of any Prime Performance Manager web interface window.

Viewing SSL Status and Print SSL Certificates

Use the following commands to view the SSL status and the SSL key and certificate pairs.

Display SSL status.

- For gateways, enter:

  ```
  /opt/CSCOppm-gw/bin/ppm ssl status
  ```

- For units, enter:

  ```
  /opt/CSCOppm-unit/bin/ppm ssl status
  ```

Print the gateway SSL certificate in X.509 format.

- For gateways, enter

```
/opt/CSCOppm-gw/bin/ppm keytool print_crt
```

- For units, enter:

```
/opt/CSCOppm-unit/bin/ppm keytool print_crt
```

List the gateway SSL key/certificate pair.

- For gateways, enter:

```
/opt/CSCOppm-gw/bin/ppm keytool list
```

- For units, enter:

```
/opt/CSCOppm-unit/bin/ppm keytool list
```

Disabling SSL

Complete the following steps to disable and remove SSL keys and certificates on a Prime Performance Manager gateway and units:

Step 1 Log into the gateway as the root or Prime Performance Manager administrator (Level 5) user.

Step 2 Stop the gateway and local unit:

```
opt/CSCOppm-gw/bin/ppm stop
```

Step 3 If remote units are connected to the gateway, log into each unit server and stop the unit:

```
opt/CSCOppm-unit/bin/ppm stop
```

Step 4 Disable SSL support on the gateway and local unit:

```
/opt/CSCOppm-gw/bin/ppm ssl disable
```

Step 5 Disable SSL on the remote units:

```
/opt/CSCOppm-unit/bin/ppm ssl disable
```

Step 6 Remove SSL keys and certificates on the gateway and local unit:

```
/opt/CSCOppm-gw/bin/ppm keytool clear
```

Step 7 Remove SSL keys and certificates on the remote units:

```
/opt/CSCOppm-unit/bin/ppm keytool clear
```

Step 8 Start the gateway and local unit:

```
opt/CSCOppm-gw/bin/ppm start
```

Step 9 Start the unit(s):

```
opt/CSCOppm-unit/bin/ppm start
```