CHAPTER 3

Configuring Security

Before you set up your server for discovering, monitoring, and configuring your Cisco network, you need to make some decisions about the level of security you need in your network monitoring.

With Cisco Prime Performance Manager, you can determine how you want users to authenticate encrypted data between the application unit and the gateway, and to limit client access to specific IP addresses.

This chapter provides information about configuring Prime Performance Manager security and limiting access to Prime Performance Manager. This chapter contains:

Configuring User Access

You can use user-based access to control the levels of access that users can have to the various functions in Prime Performance Manager. This is in addition to specifying root and non-root users.

User-based access provides multilevel, password-protected access to Prime Performance Manager features. Each user can have a unique username and password. There are five levels of access and you can assign these levels to users to allow or restrict their access to the features in Prime Performance Manager.

To configure Prime Performance Manager user access, perform the tasks in the following sections.

Required:

Optional:

Implementing Secure User Access

Before you can access the full suite of security commands in Prime Performance Manager, you must enable Prime Performance Manager user access, configure the type of security authentication you want, and add users to your user lists.

After you implement user access for Prime Performance Manager, users must log in to the system to access the:

- Prime Performance Manager web interface
- Event Editor

See Security Authentication, page 3-2 for further details.

Related Topic:

Add New User, page 6-27 - with Local Authentication enabled

Add New User, page 6-27 - with Solaris / Linux Authentication enabled

Security Authentication

Two types of security authentication are possible:

- Local authentication:

  You can create user accounts and passwords that are local to Prime Performance Manager system. With this method, you can use Prime Performance Manager user access commands to manage usernames, passwords, and access levels.

- Solaris/Linux authentication:

  Uses standard Solaris- or Linux-based user accounts and passwords, as specified in the /etc/nsswitch.conf file.

  You can provide authentication using the local /etc/passwd file; a distributed Network Information Services (NIS) system. You can use all Prime Performance Manager user access commands except:

  - `/opt/CSCOppm-gw/bin/ppm disablepass`
  - `/opt/CSCOppm-gw/bin/ppm passwordage`
  - `/opt/CSCOppm-gw/bin/ppm userpass`

PAM Setup to Check Library Version and JVM Versions

Prime Performance Manager 1.0 supports:

- Pluggable Authentication Modules (PAM) for Remote Authentication Dial in User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS+)
- Lightweight Directory Access Protocol (LDAP) authentication.

Instructions for configuring these authentication modules are provided on the Gateway install directory, /opt/CSCOppm-gw/install, and on the install directory of the Prime Performance Manager installation image as INSTALL.pam_radius.txt, INSTALL.pam_tacplus.txt, and INSTALL.pam_ldap.txt

- To ensure Java Virtual Machine (JVM) version and available Pluggable Authentication Modules (PAM) library matches, note the following:
  - If your Operating System only has 32-bit version of the PAM library, then you need to use 32-bit JVM.
  - If your Operating System only has 64-bit version of the PAM library, then you need to use 64-bit JVM.
  - If your Operating System has both 32-bit and 64-bit versions of PAM libraries, then you can use either 32-bit or 64-bit JVM.
- To check the available PAM authentication module versions based on:
  - /opt/CSCOppm-gw/install/INSTALL.pam_radius.txt, supported only in 32-bit, no 64-bit library support provided for RADIUS on Solaris, enter:

    ```
    file /usr/lib/security/pam_radius_auth.so
    ```

  - /opt/CSCOppm-gw/install/INSTALL.pam_radius.txt, supported in 32-bit and 64-bit library support provided for RADIUS on Linux, enter:

    ```
    /lib/security/pam_radius_auth.so
    /lib64/security/pam_radius_auth.so
    ```

  - Based on /opt/CSCOppm-gw/install/INSTALL.pam_tacplus.txt:

    TACACS+ on Linux, enter:

    ```
    file /lib/security/pam_tacplus_auth.so
    file /lib64/security/pam_tacplus_auth.so
    ```

    TACACS+ on Solaris, enter:

    ```
    file /usr/lib/security/pam_tacplus_auth.so
    file /usr/lib/security/sparcv9/pam_tacplus_auth.so
    ```

  - Based on /opt/CSCOppm-gw/install/INSTALL.pam_ldap.txt:

    LDAP on Linux, enter:

    ```
    file  /lib/security/pam_ldap.so
    file  /lib64/security/pam_ldap.so
    ```

    LDAP on Solaris, enter:

    ```
    file /usr/lib/security/pam_ldap.so
    file /usr/lib/security/sparcv9/pam_ldap.so
    ```

- To check JVM versions, go to:

  /opt/CSCOppm-gw/j2re/jre/bin/java -version

- To change the JVM version on Solaris:

  On Solaris, Prime Performance Manager has both 32-bit and 64-bit JVM versions. By default, Prime Performance Manager 1.0 and above enables 64-bit JVM on Solaris. To change JVM to 32-bit version, enter the following commands:

  ```
  % cd /opt/CSCOppm-gw/j2re/jre/bin
  % mv java.sgm java.64
  % mv java.32 java.sgm
  % /opt/CSCOppm-gw/bin/ppm restart
  ```

  To check if the JVM version is changed successfully, go to:

  /opt/CSCOppm-gw/j2re/jre/bin/java -version

- To check the JVM version on Linux:

  For Linux, you cannot change JVM versions. Prime Performance Manager installation program installs 64-bit JVM if the Linux runs 64-bit kernel. Prime Performance Manager installation program installs 32-bit JVM if the Linux runs 32-bit kernel.

  You need to ensure that proper version of PAM library is available on Linux that matches the kernel version.

Note Check the install subdirectory in /opt/CSCOppm-gw of Prime Performance Manager installation CD image for the notes - INSTALL.pam_radius.txt (for PAM RADIUS module) or INSTALL.pam_tacplus.txt (for TACPLUS module) and INSTALL.pam_ldap.txt (for LDAP module).

Configuring User Levels

You can configure one of four account levels for each user. Valid levels are:

1. Basic User (Level 1) Access
2. Network Operator (Level 3) Access
3. System Administrator (Level 5) Access
4. Custom User Level 1 (Level 11) and Custom User Level 2 (Level 12) Access

For more information about account levels, see Configuring Prime Performance Manager User Account Levels, page 3-6.

Configuring User Passwords

The method that you use for setting user passwords depends on the type of authentication that you configure on Prime Performance Manager system (local or Solaris/Linux).

Local Authentication

If the `ppm authtype` command is set to local, Prime Performance Manager prompts you to:

- Enter the user password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 3-6.
- Force the user to change the password at the next login. The default is to not force the user to change the password.

If the user needs to change a password, Prime Performance Manager displays an appropriate message, and prompts for the username and new password.

Solaris/Linux Authentication

If the **ppm authtype** command is set to Solaris or Linux, users cannot change their passwords by using Prime Performance Manager client. Instead, they must manage their passwords on the external authentication servers by using Solaris or Linux commands, such as *passwd*.

All new passwords take effect the next time Prime Performance Manager automatically synchronizes local Prime Performance Manager passwords with Solaris or Linux commands.

Enabling Secure User Access

To enable secure user access for Prime Performance Manager:

Step 1 Log into Prime Performance Manager server as the root user (see Starting Prime Performance Manager Server, page 2-1.

Step 2 To enable Prime Performance Manager security, the following prerequisites must be met:

- User access must be enabled.
- The authentication type must be set.
- Users must be added.

The **ppm useraccess** enable command takes you through all three stages, checking the status of:

1. **ppm useraccess**—Enabled or disabled.
2. **ppm authtype**—If you have not already set Prime Performance Manager authentication type, you must do so now.
3. **ppm adduser**—If you have already assigned users, Prime Performance Manager prompts you to either use the same user database, or create a new one. If you have not assigned users, you must do so now.

Tip For details on **ppm useraccess**, **ppm authtype**, and **ppm adduser** commands, see Appendix A, "Command Reference".

Run Prime Performance Manager useraccess enable command:

```
cd /opt/CSCOppm-gw/bin
./ppm useraccess enable
~text elided~
```

To activate your security changes on Prime Performance Manager client, restart Prime Performance Manager server using the **/opt/CSCOppm-gw/bin/ppm restart** command (see ppm restart, page A-37).

To activate your security changes on Prime Performance Manager web interface, clear the browser cache and restart the browser.

See Creating Secure Passwords, page 3-6 to further customize your Prime Performance Manager security system

Creating Secure Passwords

When setting passwords in Prime Performance Manager, the:

- Password must be at least 6 characters, and a maximum of 15 characters.
- Password cannot be identical to the username.
- New password cannot be the same as the old password.
- Prime Performance Manager does not allow users to switch back and forth between two passwords.
- Password cannot be a commonly used word. Prime Performance Manager server uses the system dictionary at /usr/share/lib/dict/words (Solaris) or /usr/share/dict/words (Linux) to determine whether a word is a commonly used word.

  To use your own dictionary, add a line to the System.properties file:

  - To disable Prime Performance Manager dictionary and allow common words, add:

    `DICT_FILE=/dev/null`

  - To use a custom dictionary, add:

    `DICT_FILE=/`*`new-dictionary`*

    where *new-dictionary* is the path and filename of the custom dictionary file, such as */users/usr11/words*. Each line in the custom dictionary must contain a single word, with no leading or trailing spaces.

Configuring Prime Performance Manager User Account Levels

This section describes the user account levels, and Prime Performance Manager client and web interface actions that are available at each level:

- Basic User (Level 1) Access, page 3-7
- Network Operator (Level 3) Access, page 3-7
- System Administrator (Level 5) Access, page 3-7
- Custom User Level 1 (Level 11) and Custom User Level 2 (Level 12) Access, page 3-7

The account level that includes an action is the lowest level with access to that action. The action is also available to all higher account levels. For example, a System Administrator also has access to all Network Operator actions.

Account levels are based on the action to be performed, not on the target network element. Therefore, if a user can perform an action on one Prime Performance Manager network element (such as deleting a node), the user can perform the same action on all similar Prime Performance Manager network elements.

Note Access to Prime Performance Manager information and downloads on Cisco.com is already protected by Cisco.com, and is not protected by Prime Performance Manager.

To configure the account level for a user, use the **ppm adduser** command, as described in Implementing Secure User Access, page 3-2, or **ppm updateuser** or **ppm newlevel** commands, as described in Enabling and Changing Users and Passwords, page 3-11.

Basic User (Level 1) Access

Basic users can view Prime Performance Manager data, load Prime Performance Manager files, and use Prime Performance Manager drill-down menus.

The following Prime Performance Manager actions in the web interfaces are available to basic users:

- View Prime Performance Manager web interface homepage
- View Reports

Network Operator (Level 3) Access

The following Prime Performance Manager actions in the web interfaces are available to network operators:

- Access all basic (Level 1) user actions
- Can view Active Alarms, Event History, Summary List
- Can access only Normal Poll node and Edit Properties option in the Actions menu

System Administrator (Level 5) Access

The following Prime Performance Manager actions in the client and web interfaces are available to system administrators:

- Accessing all basic (Level 1) user, network operator (Level 3) user access.
- Enabling and disabling reports
- Accessing all options from the Actions menu.
- Disabling, enabling and assigning temporary passwords to different user administrations.

Custom User Level 1 (Level 11) and Custom User Level 2 (Level 12) Access

The Custom User Level 1 Access and Custom User Level 2 Access by default does not have authorizations but can be customized and set permissions of all basic (Level 1) user, network operator (Level 3) and system administrator (Level 5) access.

To customize, these access levels, the user needs to edit the roles.conf file in the /opt/CSCOppm-gw/etc path in the gateway.

Automatically Disabling Users and Passwords

After you have implemented the basic Prime Performance Manager security system, you can customize the system to automatically disable users and passwords when certain conditions are met. For example, a series of unsuccessful login attempts or a specified period of inactivity).

Tip To view a list of current users and the status of user accounts, use **ppm listusers** command (see ppm listusers).

To automatically disable users and passwords:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Enter the following command:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 (Optional) To configure Prime Performance Manager to generate an alarm after a specified number of unsuccessful login attempts by a user, enter:

```
#./ppm badloginalarm number-of-attempts
```

where *number-of-attempts* is the number of unsuccessful login attempts allowed before Prime Performance Manager generates an alarm.The number of login attempts are recorded in the security log file.

Prime Performance Manager records alarms in the system security log file. The default path and filename for the system security log file is /opt/CSCOppm-gw/logs/sgmSecurityLog.txt. If you installed Prime Performance Manager in a directory other than /opt, then the system security log file resides in that directory.

By default, there can be five unsuccessful attempts before the system generates an error.

To disable this action (that is, to prevent Prime Performance Manager from automatically generating an alarm after unsuccessful login attempts), enter:

```
#./ppm badloginalarm clear
```

Step 4 (Optional) To configure Prime Performance Manager to disable a user's account automatically after a specified number of unsuccessful login attempts, enter:

```
#ppm badlogindisable number-of-attempts
```

where *number-of-attempts* is the number of unsuccessful login attempts allowed before Prime Performance Manager disables the user's account. Prime Performance Manager does not delete the user from the user list, Prime Performance Manager only disables the user's account.

By default, there can be 10 unsuccessful attempts before the system generates an error.

To re-enable the user's account, use **ppm enableuser** command.

To disable this action (that is, to prevent Prime Performance Manager from automatically disabling a user's account after unsuccessful login attempts), enter:

```
# ./ppm badlogindisable clear
```

Step 5 (Optional) Prime Performance Manager keeps track of the date and time each user last logged in. To configure Prime Performance Manager to disable a user's log in automatically after a specified number of days of inactivity, enter:

```
# ./ppm inactiveuserdays number-of-days
```

where *number-of-days* is the number of days that a user can be inactive before Prime Performance Manager disables the user's account. Prime Performance Manager does not delete the user from the user list, Prime Performance Manager only disables the user's account.

The valid range is one day to an unlimited number of days. There is no default setting.

To re-enable the user's account, use Prime Performance Manager enableuser command.

This action is disabled by default. If you do not specify the **ppm inactiveuserdays** command, user accounts are never disabled as a result of inactivity.

If you have enabled this action and you want to disable it (that is, to prevent Prime Performance Manager from automatically disabling user accounts as a result of inactivity), enter:

```
# ./ppm inactiveuserdays clear
```

Step 6 (Optional) If **ppm authtype** is set to local, you can configure Prime Performance Manager to force users to change their passwords after a specified number of days.

To configure Prime Performance Manager to force users to change their passwords after a specified number of days, enter:

```
# ./ppm passwordage number-of-days
```

where *number-of-days* is the number of days allowed before users must change their passwords.

Note You must have changed your password at least once for the **ppm passwordage** command to properly age the password.

The valid range is one day to an unlimited number of days. There is no default setting.

Prime Performance Manager starts password aging at midnight on the day that you set the value. For example, if you use the **ppm passwordage** command to set the password age to one day (24 hours), the password begins to age at midnight and expires 24 hours later.

This action is disabled by default. If you do not specify the **ppm passwordage** command, users never need to change their passwords.

If you have enabled this action and you want to disable it (that is, prevent Prime Performance Manager from forcing users to change passwords), enter:

```
# ./ppm passwordage clear
```

Note If **ppm authtype** is set to Solaris or Linux, you cannot use the **ppm passwordage** command. Instead, you must manage passwords on the external authentication servers.

Step 7 (Optional) To configure Prime Performance Manager to automatically disconnect a web interface after a specified number of minutes of inactivity, enter:

```
# ./ppm clitimeout number-of-minutes
```

where *number-of-minutes* is the number of minutes a client can be inactive before Prime Performance Manager disconnects the client.

The valid range is one minute to an unlimited number of minutes. There is no default value.

This action is disabled by default. If you do not specify the **ppm clitimeout** command, clients are never disconnected as a result of inactivity.

If you have enabled this action and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the following command:

```
# ./ppm clitimeout clear
```

Manually Disabling Users and Passwords

As described in the Automatically Disabling Users and Passwords, page 3-7, you can customize Prime Performance Manager to automatically disable users and passwords when certain conditions are met. However, you can also manually disable Prime Performance Manager users and passwords whenever you suspect that a security breech has occurred.

Note You can add new user and password from Prime Performance Manager web interface, see Add New User, page 6-27 for more details.

To disable Prime Performance Manager users and passwords:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Enter:

```
# cd /opt/CSCOppm-gw/bin
```

Step 3 (Optional) To delete a user entirely from Prime Performance Manager user access account list, enter:

```
# ./ppm deluser username
```

where *username* is the name of the user.

If you later decide to add the user back to the account list, you must use **ppm adduser** command.

Step 4 (Optional) If **ppm authtype** is set to local, you can disable a user's password. To disable a user's password, enter:

```
# ./ppm disablepass username
```

where *username* is the name of the user. Prime Performance Manager does not delete the user from the account list, Prime Performance Manager only disables the user's password.

Note If **ppm authtype** is set to Solaris or Linux, you cannot use the **ppm disablepass** command. Instead, you must manage passwords on the external authentication servers.

The user must change the password the next time they log in.

You can also re-enable the user's account with the same password, or with a new password:

- To re-enable the user's account with the same password as before, use the **ppm enableuser** command.
- To re-enable the user's account with a new password, use the **ppm userpass** command.

Step 5 (Optional) To disable a user's account, but not the user's password, enter:

```
# ./ppm disableuser username
```

where *username* is the name of the user.

Note If **ppm authtype** is set to Solaris or Linux, you must be logged in as the root user, to enter this command.

Prime Performance Manager does not delete the user from the account list; Prime Performance Manager only disables the user's account. The user cannot log in until you re-enable the user's account:

- To re-enable the user's account with the same password as before, use the **ppm enableuser** command.
- To re-enable the user's account with a new password, use the **ppm userpass** command.

Enabling and Changing Users and Passwords

Prime Performance Manager also enables you to re-enable users and passwords, and change user accounts.

To enable and change users and passwords:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Enter the following command:

```
# cd /opt/CSCOppm-gw/bin
```

Step 3 (Optional) To re-enable a user's account, which had been disabled either automatically by Prime Performance Manager, enter the following command:

```
# ./ppm enableuser username
```

where *username* is the name of the user. Prime Performance Manager re-enables the user's account with the same password as before.

Note If **ppm authtype** is set to Solaris or Linux, you must be logged in as the root user, to enter this command.

Step 4 (Optional) If **ppm authtype** is set to local, you can change a user's password, or re-enable the user's account with a new password, if the user's account had been disabled automatically by Prime Performance Manager. To change a password or to re-enable a user's account with a new password, enter:

```
# ./ppm userpass username
```

where *username* is the name of the user.

Prime Performance Manager prompts you for the new password. When setting the password, follow the rules and considerations in the Creating Secure Passwords, page 3-6.

If the user's account has also been disabled, Prime Performance Manager re-enables the user's account with the new password.

Note If **ppm authtype** is set to Solaris or Linux, you cannot use the **ppm userpass** command. Instead, you must manage passwords on the external authentication servers.

Step 5 (Optional) To change a user's account level and password, enter the following command:

```
# ppm updateuser username
```

where *username* is the name of the user.

Note If **ppm authtype** is set to Solaris or Linux, you must be logged in as the root user, to enter this command.

Prime Performance Manager prompts you for the new account level.

If **ppm authtype** is set to local, Prime Performance Manager also prompts you for the user's new password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 3-6.

Step 6 (Optional) To change a user's account level, but not the user's password, enter the following command:

```
# ./ppm newlevel username
```

where *username* is the name of the user.

Prime Performance Manager prompts you for the new account level.

Displaying a Message of the Day

You can use Prime Performance Manager to display a user-specified Prime Performance Manager system notice called the Message of the Day. You can use the Message of the Day to inform users of important changes or events in Prime Performance Manager system.

If you enable the Message of the Day, it appears whenever a user attempts to launch a client.

The Message of the Day also allows you to exit Prime Performance Manager Web User Interface before starting it in certain scenarios. If the user accepts the message, the client launches. If the user declines the message, the client does not launch.

To display the Message of the Day dialog box:

- Launch a web interface. If there is a message, the Message of the Day dialog box appears.

To configure Prime Performance Manager to display the Message of the Day:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Enter the following commands:

```
cd /opt/CSCOppm-gw/bin
./ppm motd enable
```

Prime Performance Manager displays:

```
Enter location of the message of the day file: [/opt/CSCOppm-gw/etc/motd]
```

Step 3 Press **Enter to accept the default value**; or type a different location and press **Enter**.

when a user login to Prime Performance Manager web interface, Prime Performance Manager displays:

```
Last Updated: MM:DD:YYYY Hrs:Sec AM
Message of the day
```

Step 4 **Accept** or **Decline** the Message of the day. If you accept the message, you are logged into Prime Performance Manager Web Interface.

To create the message text (the first time) or edit the existing text, enter:

```
./ppm motd edit
```

To display the contents of the Message of the Day file, enter:

```
./ppm motd cat
```

To disable the Message of the Day file, enter:

```
./ppm motd disable
```

Listing All Currently Defined Users

To list all currently defined users in Prime Performance Manager User-Based Access account list:

Note You can also view user account information on Prime Performance Manager User Accounts web page, refer User Management Table, page 6-28 for more details.

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 List all users:

```
./ppm listusers
```

Prime Performance Manager displays the following information for each user:

- Username
- Last time the user logged in
- User's account access level
- User's current account status, such as Account Enabled or Password Disabled

To list information for a specific user, enter:

```
./ppm listusers username
```

where *username* is the name of the user.

Displaying the Contents of the System Security Log

To display the contents of the system security log with PAGER:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Display the security log contents:

```
./ppm seclog
```

The following security events are recorded in the log:

- All changes to system security, including adding users
- Login attempts, whether successful or unsuccessful, and logoffs
- Attempts to switch to another user's account, whether successful or unsuccessful
- Attempts to access files or resources of higher account level
- Access to all privileged files and processes
- Operating system configuration changes and program changes, at the Solaris level
- Prime Performance Manager restarts
- Failures of computers, programs, communications, and operations, at the Solaris level

Step 4 Clear the log, by entering:

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

The default path and filename for the system security log file is */opt/CSCOppm-gw/logs/sgmSecurityLog.txt*. If you installed Prime Performance Manager in a directory other than */opt*, then the system security log file is located in that directory.

Note You can also view the system security log on Prime Performance Manager System Security Log web page. For more information, see Viewing the Security Log, page 6-10.

Disabling Prime Performance Manager User-Based Access

To completely disable Prime Performance Manager User-Based Access:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Disable user-based access:

```
./ppm useraccess disable
```

Prime Performance Manager user access is disabled the next time you restart Prime Performance Manager server (using the ppm restart command).

Enabling SSL Support on Gateway in Prime Performance Manager

Secure Socket Layer (SSL) support is enabled in both Gateway and Unit on Prime Performance Manager. The Unit establishes a connection with the Gateway as a client and after establishing a connection, the Gateway connects to the Unit as a client.

To stop both the gateway and local unit processes run the **ppm stop** command.

If any remote units are installed, run the **ppm stop** command to stop the remote units.

To enable SSL support in Prime Performance Manager:

Step 1 Use one of the following command to install an SSL key/certificate pair in Prime Performance Manager

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

The following prompts appear:

- `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]`

Step 2 Enter these details

Prime Performance Manager generates the following files on the Prime Performance Gateway:

- /opt/CSCOppm-gw/etc/ssl/server.key is Prime Performance Manager gateway's private key. Ensure that unauthorized personnel cannot access this key.
- /opt/CSCOppm-gw/etc/ssl/server.crt is the self-signed SSL certificate.
- /opt/CSCOppm-gw/etc/ssl/server.csr is a certificate signing request (CSR). It is not used if you are using a self-signed SSL certificate.

To install a new SSL key and a self-signed certificate on the Prime Performance units

Step 1 Run the following command

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

This command must be run on all units that will be connecting to the SSL-enabled Gateway.

The following prompts appear:

- `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]`

Step 2 Enter these details

Prime Performance Manager generates the following files on the Prime Performance Unit:

- /opt/CSCOppm-unit/etc/ssl/server.key is Prime Performance Manager unit's private key. Ensure that unauthorized personnel cannot access this key.
- /opt/CSCOppm-unit/etc/ssl/server.crt is the self-signed SSL certificate.
- /opt/CSCOppm-unit/etc/ssl/server.csr is a certificate signing request (CSR). It is not used if you are using a self-signed SSL certificate.

Step 3 Import the SSL certificates on the Gateway and Units:

- To import the unit certificate on the gateway, copy the /opt/CSCOppm-unit/etc/ssl/server.crt to a temporary location on the gateway machine, i.e. /tmp/server.crt. Then import the unit certificate by running the following command:

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

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

- To import the gateway certificate on the unit, copy the /opt/CSCOppm-gw/etc/ssl/server.crt to a temporary location on the unit machine, that is, /tmp/server.crt. Then import the gateway certificate by running the following command:

  `/opt/CSCOppm-unit/bin/ppm certtool import` *alias* **`-file`** *filename*

  Where *alias* is a string that is an alias for the certificate file and *filename* is the full pathname for the certificate file, i.e. /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 connect to.

Step 4 After importing, run **`/opt/CSCOppm-gw/bin/ppm ssl enable`** if its on the gateway and run **`/opt/CSCOppm-unit/bin/ppm ssl enable`** if its on the units.

Step 5 Restart the Prime Performance Manager gateway and the Prime Performance Manager units.

Note User should re-install the cross-launch in Prime Network (ANA) after enabling/disabling SSL. This ensures the cross launch links to be updated (example, change "https://" from or to "http://"). Refer Viewing Prime Network Tab Details, page 6-19

Related Topic:

Exporting an SSL Certificate, page 3-17

Viewing Detailed Information About an SSL Certificate, page 3-17

Managing SSL Support in Prime Performance Manager, page 3-17

Disabling SSL Support in Prime Performance Manager, page 3-18

Exporting an SSL Certificate

If you have implemented Secure Sockets Layer (SSL) support in your Prime Performance Manager system, you can export SSL certificates that have been imported to Prime Performance Manager Gateway or Unit.

To export a SSL certificate, run 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.

Viewing Detailed Information About an SSL Certificate

If you implemented Secure Sockets Layer (SSL) support in your Prime Performance Manager system, you can view detailed information about SSL certificates that were imported to Prime Performance Manager Gateway or Unit.

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.

Managing SSL Support in Prime Performance Manager

Managing SSL support in Prime Performance Manager is done by the following set of commands:

- To view the status of SSL support (enabled/disabled) and the list of SSL keys and certificates available in Prime Performance Manager, use the following commands:

  Gateway Commands:

  /opt/CSCOppm-gw/bin/ppm ssl status
  or
  /opt/CSCOppm-gw/bin/ppm sslstatus

  Unit Commands:

  /opt/CSCOppm-unit/bin/ppm ssl status
  or
  /opt/CSCOppm-unit/bin/ppm sslstatus

- To Print Prime Performance Manager server's SSL certificate in X.509 format, use the following command:

  Gateway Command:

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

  Unit Command:

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

- To list the SSL key/certificate pair on Prime Performance Manager server, use the following command:

  Gateway Command:

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

  Unit Command:

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

Disabling SSL Support in Prime Performance Manager

To disable and remove SSL keys and certificates support in Prime Performance Manager gateway and units, use these commands:

Note Before disabling or removing SSL support, stop both the gateway and local unit processes by running the opt/CSCOppm-gw/bin/ppm stop command.

- To disable SSL support in Prime Performance Manager gateway and units, use the following commands:

  Gateway Command:

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

  Unit Command:

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

- To remove all SSL keys and certificates from Prime Performance Manager gateway and units, use the following commands:

  Gateway Command:

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

  Unit Command:

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

Limiting Prime Performance Manager Client Access to Prime Performance Manager Server

By default, when you first install Prime Performance Manager, all Prime Performance Manager client IP addresses can connect to Prime Performance Manager server. However, you use Prime Performance Manager to limit client access to the server by creating and maintaining the *ipaccess.conf* file.

You can create the *ipaccess.conf* file and populate it with a list of Prime Performance Manager client IP addresses that can connect to Prime Performance Manager server. Prime Performance Manager allows connections from only those clients and the local host.

If the file exists but is empty, Prime Performance Manager allows connections only from the local host. (Prime Performance Manager always allows connections from the local host.)

When you first install Prime Performance Manager, the *ipaccess.conf* file does not exist and Prime Performance Manager allows all client IP addresses to connect to Prime Performance Manager server.

To create the *ipaccess.conf* file and work with the list of allowed client IP addresses:

Step 1 Log into Prime Performance Manager server as the root:

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Create the *ipaccess.conf* file:

- To create the *ipaccess.conf* file and add a client IP address to the list, enter:

  ```
  ./ppm ipaccess add
  ```

- To create the *ipaccess.conf* file and open the file to edit it directly, enter:

  ```
  ./ppm ipaccess edit
  ```

The default directory for the file is located in Prime Performance Manager installation directory:

- If you installed Prime Performance Manager in the default directory, */opt*, then the default directory is */opt/CSCOppm-gw/etc*.
- If you installed Prime Performance Manager in a different directory, then the default directory is located in that directory.

In the *ipaccess.conf* file, begin all comment lines with a pound sign (#).

All other lines in the file are Prime Performance Manager client IP addresses, with one address per line.

Wildcards (*) are allowed, as are ranges (for example, 1-100). For example, if you input the address ***.*.*.*** then all clients can connect to Prime Performance Manager server.

Step 4 After you create the *ipaccess.conf* file, you can use the full set of Prime Performance Manager ipaccess keywords to work with the file. The keywords are:

- `clear`—Remove all client IP addresses from the *ipaccess.conf* file, and allow connections from any Prime Performance Manager client IP address.
- **`list`**—List all client IP addresses currently in the *ipaccess.conf* file. If no client IP addresses are listed (that is, the list is empty), connections from any Prime Performance Manager client IP address are allowed.

- **rem**—Remove the specified client IP address from the *ipaccess.conf* file.
- sample—Print out a sample *ipaccess.conf* file.

For more information, see ppm ipaccess, page A-25.

Any changes you make to the *ipaccess.conf* file take effect when you restart Prime Performance Manager server.

Backing Up or Restoring Prime Performance Manager Files

Backup and Restore function in Prime Performance Manager allows you to retrieve user accounts and security-related parts of Prime Performance Manager data files from the previous night's backup.

Backup and Restore should ideally be performed in sets at the same clock time. Sets consists of a Gateway and its units.

Note When Backup is not performed in sets, there is an potential for data not in synchronization between the Gateway and its units.

Below are the backup and restore steps followed on a gateway and a unit:

1. Backup performed on both the gateway and unit at the same time (or nearly so)
2. Backup restored to the gateway first
3. Backup restored to the unit
4. Gateway started
5. Unit started

Below are the backup and restore steps followed on a gateway and multiple units:

1. Backup performed on the gateway and all units at the same time (or nearly so)
2. Backup restored to the gateway first
3. Backup restored to each unit. These restores can be done in parallel.
4. Gateway started
5. Units started. the units can be started serially or in parallel.

Prime Performance Manager v1.0 supports backup and restore on the same machine. For example, taking a backup on unit 1 and restoring to unit 2 is not supported. Taking a backup on a gateway with one IP address and restoring to a gateway with a different IP address is not supported.

System responsiveness may temporarily degrade during backup for very large scale networks.

To restore the security-related Prime Performance Manager data files:

Step 1 Log in as the root user

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the /bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Restore the security-related data:

```
./ppm restore
```

Prime Performance Manager restores the data.

Prime Performance Manager automatically backs up all Prime Performance Manager data files to Prime Performance Manager installation directory daily at same clock time.

To change the time at which Prime Performance Manager automatically backs up files, log in as the root user and change the *root crontab* file:

- **crontab -l** lists cron jobs.
- **crontab -e** opens up an editor so you can make changes and save them.

This section contains these topics:

Backing Up Prime Performance Manager Data Files

To manually back up Prime Performance Manager data files at any time on a Solaris or Linux server:

Step 1 Log in as the root user.

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Back up Prime Performance Manager files:

```
./ppm backup
```

Prime Performance Manager backs up the data files in the installation directory.

If you installed Prime Performance Manager in the default directory, */opt*, then the default backup directory is also */opt*. If you installed Prime Performance Manager in a different directory, then the default backup directory is that directory.

Changing the Backup Directory

To change the directory in which Prime Performance Manager stores its nightly backup files:

Step 1 Log in as the root user.

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Change the backup directory location:

`./ppm backupdir` *directory*

where *directory* is the new backup directory.

If the new directory does not exist, Prime Performance Manager does not change the directory, but issues an appropriate warning message.

Setting the Number of Backup Days

To set the number of days that Prime Performance Manager saves backup files:

Step 1 Log in as the root user.

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Change the number of backup days (default is 1):

```
./ppm backupdays
```

Step 4 Enter a value for the number of days from 1 to 30.

Prime Performance Manager will save backup files for the number of days that you entered. In this example, Prime Performance Manager saves backup files for the last five days, and deletes backup files that are older than five days.

Restoring Prime Performance Manager Data Files

Prime Performance Manager supports backup and restore on the same machine. For example, taking a backup on unit 1 and restoring to unit 2 is not supported. Taking a backup on a gateway with one IP address and restoring to a gateway with a different IP address is not supported.

Note Prime Performance Manager data restore can be made on the same server the backup was taken.

To restore Prime Performance Manager data files from a previous backup:

Step 1 Log in as the root user.

For details about the root user, see Becoming the Root User, page 2-2

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Restore Prime Performance Manager data files:

```
./ppm restore
```

Prime Performance Manager restores the data files.

Note If the number of backup days has been set to more than one day (see Setting the Number of Backup Days, page 3-22), Prime Performance Manager will prompt you for a server backup file restore from as there is no client backups.

Warning **Do not interrupt this command. Doing so can corrupt your Prime Performance Manager data files.**

ppm restore command provides optional keywords that you use to restore only selected Prime Performance Manager data files, such as log files, report files, or security files. For more information, see Backing Up or Restoring Prime Performance Manager Files, page 3-20.