Managing Users and Security

Before you set up the Prime Performance Manager gateway and begin discovering and monitoring your network, you need to decide the user security levels, that is, which users will be allowed to which Prime Performance Manager functions.

Prime Performance Manager allows you to decide how users are authenticated, what actions they can perform, and which client IP addresses can access Prime Performance Manager gateways and units.

The following topics provide information about setting up user access and security, configuring user passwords, and managing Prime Performance Manager users:

- Setting Up User Access and Security, page 6-1
- Managing Users and User Security, page 6-15

Tip If you have a collocated single server and only want to enable user access, you can use the ppm uaenable command. This command does everything for you except create the first admin level user. The command will set up everything else including configuring the SSL keys, and swapping the keys between the gateway and unit, and prompting you to enter the first admin level user. For more information, see ppm uaenable, page B-117.

Note If you integrate Prime Performance Manager with Cisco Prime Central, all user management functions are handled by Prime Central, and the user and security options are not displayed in Prime Performance Manager. After integration, users access all Cisco Prime domain managers, such as Prime Performance Manager, Prime Network, and others, using a single login. Information provided in these topics are useful, however, particularly user roles, which will be assigned in Prime Central. An understanding of user password configuration is also helpful. For more information about integrating Prime Performance Manager with Prime Central, see Chapter 4, “Importing Devices From Other Cisco Prime Applications.”

Setting Up User Access and Security

Enabling user access allows you to control what users can view and perform in Prime Performance Manager. User access provides multilevel, password-protected access to Prime Performance Manager functions. Five access roles are available, and you can assign these roles to users to allow or restrict their access to Prime Performance Manager features and functions.

Table 6-1 lists the user access task flow and topics providing the steps or additional information.

Table 6-1 Setting Up and Managing User Access and Security

User Access Task	For More Information
User and Security Setup Tasks	
Enable Secure Sockets Layer on gateways and units. This task is required.	Enabling SSL on Gateways and Units, page 6-2
Determine how users will be authenticated.	User Authentication, page 6-8
Configure user passwords.	Configuring User Passwords, page 6-9
Review secure password requirements.	Modifying the Password Policy, page 6-9
Review user roles.	User Security Levels, page 6-10
Enable user access.	Enabling Secure User Access, page 6-11
Disable user-based access.	Disabling Secure User Access, page 6-12
Add new users.	Adding New Users, page 6-15
User and Security Management Tasks	
Edit user information.	Displaying User Information, page 6-16
Define the reports users can access.	Filtering Reports Assigned to Individual Users, page 6-20
Change user passwords.	Changing User Passwords, page 6-20
Edit user security settings.	Editing User Security Settings, page 6-21
Manually disable users and passwords.	Manually Disabling Users and Passwords, page 6-22
Enable user accounts and passwords.	Enabling User Accounts and Passwords Using the CLI, page 6-24
List currently defined users.	Listing Currently Defined Users, page 6-27
Display the system security log.	Displaying the System Security Log, page 6-27

Enabling SSL on Gateways and Units

To enable user access SSL must be enabled on Prime Performance Manager gateways and units. To enable SSL, you generate the SSL key and certificate for the gateway and each connected unit, then import corresponding keys and certificates to the gateway and units. In other words, 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 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.

Note If you are purchasing an SSL certificate from a third-party Certificate Authority vendor, complete the Enabling Third Party CA Certificates for Cisco Prime Performance Manager, page 6-6, before you enable SSL on the gateway and unit.

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

- Enabling SSL on a Gateway or Collocated Gateway and Unit, page 6-3
- Enabling SSL on Remote Units, page 6-4

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.
- 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.
- 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 3 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 6-4. 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 into 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 Enable SSL on gateway:

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

Step 5 Execute the autoExchangeSSL.sh script to exchange SSL certificates between the gateway and remote unit:

```
/opt/CSCOppm-gw/bin/autoExchangeSSL.sh
```

Step 6 Enter the path to the gateway certificate:

```
Please Enter Gateway( ppm64-v6.cisco.com) Node Certificate Path:
[/opt/<gateway>/etc/ssl/server.crt]
```

Step 7 Enter the remote unit IP address:

```
Please Enter Remote Node IP: nnn.nnn.nnn.nnn
```

Step 8 Enter the remote unit username and password:

```
Please Enter SSH username for Remote Node(10.74.125.192):  [root]
Please Enter SSH Password for Remote Node(10.74.125.192):
SSH Connection Test successful!
```

Step 9 Enter the path to the unit certificate:

```
Please Enter Certificate Path for Remote Node(10.74.125.192)
[/opt/<unit>/etc/ssl/server.crt]
```

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:

```
#################Remote Node(nnn.nnn.nnn.nnn) import Gateway (gatewayIP)
Certificate...#################
```

```
Remote Node (unitIP) import Gateway (gateway) Certificate was added to keystore
successful!
################ Gateway(gateway) import Remote Node(unitIP)
Certificate...#################
localsever(gateway) import Remote Node(unitIP) Certificate was added to keystore
successful !
```

Step 10 Restart the gateway:

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

Step 11 Restart the remote unit:

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

Related Topics:

Exporting SSL Certificates, page 6-5

Displaying SSL Status, page 6-5

Disabling SSL, page 6-6

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.

Displaying SSL Status

To display SSL status:

- For gateways, enter:

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

- For units, enter:

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

Printing SSL Certificates

To 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
```

Displaying the SSL Key and Certificate

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 from Prime Performance Manager gateways and units:

Step 1 Log into the gateway as the root or Prime Performance Manager administrator 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
```

Enabling Third Party CA Certificates for Cisco Prime Performance Manager

To enable third-party Certificate Authority (CA) SSL certificates for your website, you must purchase certificates issued by a third-party CA vendor such as Symantec (previously VeriSign), DigiCert, GoDaddy or other third party vendor. When you order the certificate, the vendors might ask you to enter

the number of servers that will be secured with the certificate. This is the number of licenses you want to purchase for the certificate, or the number of web servers on which you're going to install the certificate.

To generate a self-signed key and certificate for Prime Performance Manager:

Step 1 From the Prime Performance Manager gateway, enter the following command:

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

The command generates the following files:

```
-rw-r--r--. 1  root root 1647 Jun 12 15:42 server.crt
-rw-r--r--. 1  root root 1054 Jun 12 15:42 server.csr
-rw-------. 1 root root 1675 Jun 12 15:37 server.key
-rw-r--r--. 1  root root 2973 Jun 12 15:42 sgmSslCerts
-rw-------. 1 root root 2896 Jun 12 15:42 sgmSslKey
```

where server.csr is the certificate signing request file (CSR).

Step 2 Purchase the third-party CA certificate:

a. Log into the third-party CA website and register an account to purchase your SSL certificate.

b. During the order, open the server.csr file listed above in a text editor and copy the entire content including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines.

c. Paste the content in the form that asks you to enter the CSR on the third-party CA website.

d. Enter any additional required information, then submit the purchase order.

Note When you enable SSL in Prime Performance Manager, the ppm ssl enable command also generates the above key/certificate files. However, the default CSR file is generated with a few items left empty such as: Country Name, State or Province Name, Locality Name, Organization Name. and other fields. If you request a third-party CA signed certificate, do not use the default CSR file during the purchase because it will not pass the CA validation and an SSL certificate will not be issued.

Step 3 Download the signed, third-party CA certificate:

After your SSL certificate purchase request is validated, the CA company issues you a signed SSL certificate. Depending on the vendor, you can have the signed SSL certificate sent to you by email or you can download the certificate from the vendor's website. Usually the signed SSL certificate is named <your-domain-name>.crt. (The certificate file can also have the extension DER, PEM, or CER). Save the signed SSL certificate file locally for later import into Prime Performance Manager.

Note Some CA vendors might also send you an intermediate certificate file. If so, download it and save locally.

Step 4 In Prime Performance Manager, enter the following command to import the signed third-party CA certificate:

```
/opt/CSCOppm-gw/bin/ppm keytool import_cert <cert_filename>
```

where the <cert_filename> is the signed CA certificate from the CA vendor.

Note If you received an intermediate certificate file from the CA vendor, import it before you import the above signed certificate. Contact the CA vendor for any technical support and service.

After the import, the old self-signed certificate is replaced with the imported one.

Step 5 Complete the Enabling SSL on a Gateway or Collocated Gateway and Unit, page 6-3 to configure SSL for the gateway.

The web interface is now be secured by the signed CA certificate.

Note Gateway and unit communication uses Java RMI. After SSL is enabled, the gateway and unit also uses SSL to secure the communication. However, because the unit is not open to end users, a signed CA SSL certificate is not required for gateway and unit communication. Therefore, you can still use the default Prime Performance Manager self-signed certificate for the unit servers. For details, see Enabling SSL on Remote Units, page 6-4.

User Authentication

After you implement user access for Prime Performance Manager, users must log into the system to access the Prime Performance Manager web interface and CLI commands. Security authentications include:

- Cisco Prime Central single signon (SSO) authentication. Prime Central SSO is enabled after you integrate Prime Performance Manager with Prime Network.
- 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

Authentication Through PAM, TACACS+, and LDAP

Prime Performance Manager can use authentication through Pluggable Authentication Modules (PAM) for Remote Authentication Dial in User Service (RADIUS), Terminal Access Controller Access-Control System (TACACS+), Lightweight Directory Access Protocol (LDAP), and Microsoft Active Directory authentication.

Instructions for configuring these authentication modules are provided in the following files:

- INSTALL.pam_radius.txt
- INSTALL.pam_tacplus.txt
- INSTALL.pam_ldap.txt.
- INSTALL.pam_msactivedir.txt

These files are located in the Prime Performance Manager gateway installation directory (/opt/CSCOppm-gw/install by default). Cisco provides the configuration information only as general guidance. Any specific PAM deployment issues are beyond the scope of Cisco support.

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, Solaris/Linux, or Prime).

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 Modifying the Password Policy, page 6-9.
- 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.

Modifying the Password Policy

By default, Prime Performance Manager enables password requirements that ensure the security of your system. Although not recommended, you can disable any or all of these requirements by completing the following steps:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 On the Users screen, click **Password Policy**.

Step 4 By default, all password security options are enabled. Disable any that you do not want enforced:

- Password minimum length must be *n* characters.

  The default is 8. You can set a value ranging from 0 through 127.
- Password maximum length must be *n* characters.

  The default is 80. You can set a value ranging from 0 through 127.

- Password cannot be a username or the reverse of a username.
- Password cannot contain “cisco” or any variations including “ocsic”, any capitalized letter variant therein, or by substituting '1', '|', or '!' for i, '0' for 'o', or '$' for 's'.
- No character can be repeated more than two consecutive times in the password.
- Password must contain at least one character from the three character classes:
  - upper case
  - lower case
  - digits and special characters
- Password cannot contain ascending or descending characters.
- Password cannot be the same as the previous five passwords.
- Password cannot contain a dictionary word.

  By default, the Prime Performance Manager gateway 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:

  `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.

Step 5 When finished, click **Save**.

User Security Levels

Prime Performance Manager provides five default user roles and two user roles that you can customize. 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 user also has access to all Network Operator user 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, you can use the **ppm adduser** command, as described in User Authentication, page 6-8, or **ppm updateuser** or **ppm newlevel** commands, as described in Enabling User Accounts and Passwords Using the CLI, page 6-24.

Table 6-2 Prime Performance Manager User Levels

Role	Access
Basic User	• View Prime Performance Manager data, load Prime Performance Manager files, and use Prime Performance Manager drill-down menus. • View Prime Performance Manager web interface homepage. • View Reports.
View Administrator	• View Prime Performance Manager data, load Prime Performance Manager files, and use Prime Performance Manager drill-down menus. • View Prime Performance Manager web interface homepage. • View Reports. • Create and edit views.
Network Operator	• Access all basic user actions. • View alarms and events. • Access only the Normal Poll and Edit Properties options in the device Actions menu.
System Administrator	• Access all basic user and network operator user functions. • Enable and disable reports • Access all options from the device Actions menu. • Disable, enable, and assign temporary passwords to different user administrations.
Custom Level 1 Custom Level 2	The Custom Level 1 and Custom Level 2 by default do not have authorizations. However, they can be customized and set permissions from basic user, network operator, and system administrator roles. To customize, these access levels, edit the roles.conf file in the /opt/CSCOppm-gw/etc.

Enabling Secure User Access

Secure user access to Prime Performance Manager can be enabled by integrating with Prime Central and managing users through Prime Central, or by enabling secure user access from Prime Performance Manager. For information about integrating Prime Performance Manager with Prime Central, see Chapter 4, "Importing Devices From Other Cisco Prime Applications."

To enable secure user access for Prime Performance Manager that is not integrated with Prime Central:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging In as the Root User, page 2-1.

Step 2 If SSL is not enabled, complete the "Enabling SSL on Gateways and Units" procedure on page 6-2.

Step 3 Run the ppm useraccess enable command:

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

After enabling user access, the ppm useraccess command calls up the authentication type and add user commands:

- ppm authtype—If you have not set Prime Performance Manager authentication type, you must set it now.
- ppm adduser—If you have created users, Prime Performance Manager prompts you to use the same user database or create a new one.

Step 4 To activate your security changes on the client, restart the Prime Performance Manager gateway:

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

Step 5 To activate the security changes on Prime Performance Manager web interface, clear the browser cache and restart the browser.

Step 6 See Modifying the Password Policy, page 6-9, to further customize your Prime Performance Manager security.

Disabling Secure User Access

Should you wish to disable Prime Performance Manager secure user access, complete the following steps:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging In as the Root User, page 2-1.

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 gateway (using the ppm restart command).

Configuring Microsoft Active Directory Authentication

You can configure Prime Performance Manager to use Microsoft Active Directory for authenticating users using PAM and LDAP.

To configure Prime Performance Manager to use Microsoft Active Directory for authenticating users:

Step 1 Log into the Active Directory server.

Step 2 Launch Active Directory and display the New Users and Computers window.

Step 3 Create a PPM Bind bind user directly under the domain, ppm.local.

Note This procedure uses ppm.local as an example domain. The domain can have any name of your choosing. The user should not belong to any groups.

Step 4 In the New Object - User wizard, enter the following:

- First name—PPM
- Last name—Bind
- Full name—PPM Bind
- User logon name—PPMBind @ppm.local
- User logon name (pre-Windows 2000)—PPMBind.

Step 5 Click **Next**.

Step 6 In the next wizard panel, enter the following:

- Password—Enter Cisco123.
- Confirm password—Enter Cisco123.
- Check the following options:
  - User cannot change password
  - Password never expires

  Do not check the other options.
- User logon name—PPMBind @ppm.local
- User logon name (pre-Windows 2000)—PPMBind.

Step 7 At the command prompt, enter **dsquery** to verify the user is configured properly. The following response should appear:

```
C:\Documents and Settings\Administrator.LDAP-MBARUCH>dsquery user -namne PPM*"CN=PPM
Bind,DC=ppm,DC=local"
C:\Documents and Settings\Administrator.LDAP-MBARUCH>
```

Note The dsquery command was executed on Window 2003. You might need to install users separately on other Windows versions, and the command format or syntax might differ. See the Microsoft Windows documentation for details.

Step 8 Complete the following steps to edit the ldap.conf:

```
vi /etc/ldap.conf
```

a. Add the hostname:

```
# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host LDAP-Server.cisco.com
```

b. Add the search base:

```
# The distinguished name of the search base.
base DC=ppm,DC=local
```

c. Add the bind user details. This must match the dsquery results.

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn CN=PPM Bind,DC=ppm,DC=local
```

d. Add the bind password:

```
# The credentials to bind with.
# Optional: default is no credential.
bindpw Cisco123
```

e. Update the PAM details in the # RFC 2307 (AD) mappings section:

```
pam_login_attribute sAMAccountName
pam_password ad
```

f. Verify that /etc/ldap.conf has the following:

```
# cat /etc/ldap.conf | grep -v '^[#]' | grep -v '^$'
host LDAP-Server.cisco.com
base DC=t4,DC=local
CN=PPM Bind,DC=t4,DC=local
bindpw Cisco123
timelimit 120
bind_timelimit 120
idle_timelimit 3600
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm
pam_login_attribute sAMAccountName
pam_password ad
```

Step 9 Edit the ppm-jpam file based on your OS type:

```
vi /etc/pam.d/ppm-jpam
# Change pam_unix_auth.so to pam_ldap.so
# Change pam_unix_acct.so to pam_ldap.so
# The following is for Linux 64
    auth        required  /lib64/security/pam_ldap.so
    account     required  /lib64/security/pam_ldap.so
# The following is for Linux 32
    auth        required  /lib/security/pam_ldap.so
    account     required   /lib/security/pam_ldap.so
```

Step 10 If Prime Performance Manager user access is not enabled, enable it:

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

Choose the auth mode as Linux

When you create the default user, enter **y** for the following confirmation:

```
Can't match key TestLinux in map passwd.byname. Reason: No such key in map
Could not find user in /etc/passwd or NIS.
Should User User1 be added anyway? [n] y
```

Step 11 Add the Prime Performance Manager users:

#/opt/CSCOppm-gw/bin/ppm adduser

When you create the default user, enter **y** for the following confirmation:

```
Can't match key TestLinux in map passwd.byname. Reason: No such key in map
Could not find user in /etc/passwd or NIS.
Should User User1 be added anyway? [n] y
```

Users created on the MS AD server but not added to Prime Performance Manager can still log into Prime Performance Manager but only with the basic access level.

Step 12 Verify the user login

a. Connect to https://servername:4440.

b. Test the user login using any username/password configured on the MS-AD server.

Managing Users and User Security

Prime Performance Manager allows you to add and manage users through the web interface. Before you can do this, however, user access must be enabled. A System Administrator user must be created during installation or post-installation, using Prime Performance Manager CLI as root.

A web user with System Administrator permissions can add or delete users, modify user passwords and roles and access levels. In addition, report policies can be assigned to users specifying what reports they are allowed to see.

These actions are covered in the following topics:

- Adding New Users, page 6-15
- Displaying User Information, page 6-16
- Editing User Information, page 6-18
- Creating User Groups, page 6-18
- Filtering Reports Assigned to User Groups, page 6-19
- Filtering Reports Assigned to Individual Users, page 6-20
- Changing User Passwords, page 6-20
- Editing User Security Settings, page 6-21
- Manually Disabling Users and Passwords, page 6-22
- Enabling User Accounts and Passwords Using the CLI, page 6-24
- Creating Messages of the Day, page 6-25
- Listing Currently Defined Users, page 6-27
- Displaying the System Security Log, page 6-27
- Disabling Secure User Access, page 6-12

Adding New Users

Administrator users can add new users to Prime Performance Manager. To add a new user:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 In the Users window, click the **Add User** tool.

Step 4 Complete the new user information. The options that appear depend on whether you enabled local authentication or use another type of user authentication. (See User Authentication, page 6-8.)

- User Name—Enter the new username.
- First Name—Enter the user first name.
- Last Name—Enter the user's last name.

Note A star "*" character is not permitted in the user names.

- Role—Enter the user authentication role for the user. The valid values are:
  - Basic User
  - Network Operator
  - System Administrator
  - View Administrator
  - Custom Level 1
  - Custom Level 2

Note For a description of security levels, see User Security Levels, page 6-10.

- User Group—Allows you to assign a user to a user group. To do this, you must create a user group. See Creating User Groups, page 6-18.
- Home View—Allows you to assign a home view to the user. Views created in the Prime Performance Manager gateway appear in the Home View drop down list. The view you assign is the one the user sees when he or she logs into Prime Performance Manager,
- Password (local authentication only)—Enter the user password.
- Confirm Password (local authentication only)—Retype the password to confirm the new password.
- Email—(optional) Enter the user's e-mail address.
- Phone—(optional) Enter the user's phone number.
- Customer—(optional) Enter the user's customer name.
- Account Number—(optional) Enter the user's account number.
- Tenant Name—If multi-tenancy is implemented, allows you to associated the user to a tenant account.
- Force user to reset password at login? (local authentication only)—If selected, the user will be required to change the password the next time they log in.

Step 5 Click **Save**.

Displaying User Information

After you add users, you can display the user information at any later point:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

The Users table displays the following information:

- User Name—The Prime Performance Manager user for whom a user-based access account is set up.
- First Name—The user's first name.

- Last Name—The user's last name.

Note A star "*" character is not permitted in the user names.

- User Group—The user group assigned to the user, if any.
- Home View—The home view assigned to the user, if assigned,
- Report Filter—Allows you filter reports by user. See Filtering Reports Assigned to Individual Users, page 6-20.
- Login Time—The date and time the user last logged into Prime Performance Manager.
- Role—Authentication level and number for the user. You can modify the user access level. Valid access levels and numbers include:
  - Basic User
  - Network Operator
  - System Administrator
  - View Administrator
  - Custom Level 1
  - Custom Level 2

  See Table 6-2 on page 6-11, for a description of actions each user can perform.
- Active—The current user's account status: Yes (the account is functioning normally), or No. A user account can be disabled for the following reasons:
  - A System Administrator disabled the account. See "Manually Disabling Users and Passwords" section on page 6-22 for more information.
  - Prime Performance Manager disabled the account because of too many failed attempts to log in. See the "Editing User Security Settings" section on page 6-21 for more information.
  - Prime Performance Manager disabled the account because it was inactive for too many days. See the "Editing User Security Settings" section on page 6-21 for more information.
  - Expired Password—Indicates the user's password has expired.
  - Temporary Password—Indicates the user has a temporary password.
- Tenants—If tenants are assigned to the user, there are displayed.
- Details—Allows you to display and/or edit the following optional user details by clicking the circle icon in the Details cell:
  - Email
  - Phone
  - Customer
  - Account Number

Editing User Information

To edit user information:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 In the Users window, check the box next to user whose information you want to edit.

Step 4 Click **Edit** on the Users toolbar.

Step 5 In the Edit User Information dialog box, revise any of the following information:

- First Name
- Last Name
- Email address
- Phone
- Customer Name
- Account Number
- Role
- User Group
- Home View
- Password Aging
- Tenant Name

Step 6 Click **Save**.

Creating User Groups

You can create user groups and assign users to them. You can then customize the reports that are available to the user group. For example, if you have an external customer with many individuals who want to look at the same reports, you can assign those individuals to a user group and customize the reports available to the user group.

Note Users can only be assigned to one user group.

To create a user group:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 On the Users window, click **User Groups**.

Step 4 In the User Groups window, click **Add**.

Step 5 In the Add User Group dialog box, enter the use group name. The name cannot have spaces or special characters, except hyphens and underscores.

Step 6 Enter a description in the User Group Description field.

Step 7 Click **Save**.

The new group appears in the User Groups list.

Step 8 To assign users to user groups, complete one of the following procedures:

- Adding New Users, page 6-15
- Editing User Information, page 6-18

Filtering Reports Assigned to User Groups

To assign specific reports to user groups:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 On the Users window, click **User Groups**.

Step 4 In the User Groups window, choose the user groups for which you want to filter reports.

Step 5 On the User Groups toolbar, click **Filter Reports**.

Step 6 In the Filter User Reports dialog box, expand the report trees and deselect the reports you do not want the user to access.

Step 7 If you want to provide additional report filtering:

a. Expand the report tree to the end report view. In this view, report names have a Filter icon next to the report name.

b. Click the **Filter** icon next to the report you want to filter,

c. In the Filter [report name] dialog box, choose one of the following:

– Filter Using a Group—If you choose this option, choose the group name in the Group Name list. (Processing Name is always set to default.)

– Filter Using a Report Column—If you choose this option, complete the following:

Column Name—Choose the report data item that you want to base the filter on. The items displayed depend on the report.

Operator—Enter the operator value: equals, not equal, greater than, and others.

Filter Value—Enter the filter value. For example, filter the parameter to listed in Column Name by the operation in the Operator field to the number entered here.

d. Click **Save**.

Filtering Reports Assigned to Individual Users

By default, all users can access all reports available on the gateway. To limit the reports that a user can access:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 In the Users window, choose the users for which you want to filter reports.

Step 4 On the Users toolbar, click **Filter Reports**.

Step 5 In the Edit User Reports dialog box, expand the report trees and deselect the reports you do not want the user to access.

Step 6 If you want to provide additional report filtering:

a. Expand the report tree to the end report view. In this view, report names have a Filter icon next to the report name.

b. Click the **Filter** icon next to the report you want to filter,

c. In the Filter [report name] dialog box, choose one of the following:

- Filter Using a Group—If you choose this option, choose the group name in the Group Name list. (Processing Name is always set to default.)
- Filter Using a Report Column—If you choose this option, complete the following:
- Column Name—Choose the report data item that you want to base the filter on. The items displayed depend on the report.
- Operator—Enter the operator value: equals, not equal, greater than, and others.
- Filter Value—Enter the filter value. For example, filter the parameter to listed in Column Name by the operation in the Operator field to the number entered here.

d. Click **Save**.

Note If you are member of a group and that group has reports filtered, your individual report filtering settings take priority over the group settings.

Tip To quickly clear all user report filters, click **Reset to Default**.

Changing User Passwords

Administrators can change any user password; individual users can change their own passwords.

If you want to change your own password:

Step 1 Log into Prime Performance Manager.

Step 2 From the user ID on the top right corner of the Prime Performance Manager window, choose **Change Password**.

Step 3 In the Change Password dialog box, enter the new password, then enter it again in the Confirm Password field.

Step 4 Click **OK**.

If you are an administrator and want to change a user password:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 In the Users window, select a user whose password you want to change, then click the **Reset Password** tool.

Step 4 In the Update User window, complete the following information.

- Password—Enter the password.
- Confirm Password—Retype the password to confirm the new password.
- Force user to reset password at login?—Select if you want the user to change their password at their next log in.

Step 5 Click **Save**.

Note You can also change user passwords using the ppm userpass command. See ppm userpass, page B-120.

Editing User Security Settings

You can edit user security settings that to automatically disable users and passwords when certain conditions are met, for example, control the number of failed logins before an alarm is issued, the number of failed logins before a user disabled, and other security parameters.

To edit user security settings:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**.

Step 3 On the Users screen, click **Security Settings**.

Step 4 In the Security Settings window, edit any of the following:

- Number of Failed Logins Before Alarm—Sets the number of failed logins before an alarm is raised. The default is 5. The range is 1-10. Entering 0 disables this setting. (To provision this parameter using the CLI, see ppm badloginalarm, page B-18.)
- Number of Failed Logins Before Account Disabled—Sets the number of failed logins before the user's account is disabled. The default is 10. The range is 1-10. Entering 0 disables this setting. (To provision this parameter using the CLI, see ppm badlogindisable, page B-19.)

Note Prime Performance Manager restricts users who attempt to log in from different IP addresses within ten-minute period. A threshold is calculated based upon the number of IP addresses that made unsuccessful login attempts. Prime Performance Manager calculates the maximum number of login attempt number for a given user from those IP Addresses.

- Number of Days Before Disabling Inactive Users—Sets the number of days of inactivity before a user is disabled. The valid range is 1-365. The default is 0; inactive users will never be disabled. (To provision this parameter using the CLI, see ppm inactiveuserdays, page B-46.)
- Number of Days Before Forcing a Password Change—Sets the number of days before the user must change their password. The valid range is 1-365. The default is 0; users will never be forced to change their password. (To provision this parameter using the CLI, see ppm passwordage, page B-67.)
- Number of Minutes Before Disabling Inactive Clients—Sets the number of minutes before disabling an inactive client. The valid range is 1-120. The default is 0; inactive clients are never disabled. (To provision this parameter using the CLI, see ppm clitimeout, page B-23.)
- Password Notification Early Notification Days—Sets the number of days before password expiration when a notification is sent to the user. The default is 15 days. The range is 0-30.
- Single Session—Defines the number of active sessions a user can create:
  - Enable—Only a single session is allowed per user. If a user logs into a second web interface session, the first session is ended.
  - Disable—(Default) Disables the single session per user restriction. The user can log in as the same user from multiple web interfaces.
  - Block—Only a single session is allowed per user. If a user attempts to log into a second web interface session, they are blocked until they close the first session.
- Restrict Password Changes—Provides restrictions on the password change frequency:
  - Password Change Interval—Specifies with time interval, between 1 and 745 hours, within which the password change restriction applies. 48 hours is the default.
  - Number of Password Changes per Interval—Specifies the permissible number of password changes, between 1 and 10, allowed within the time interval specified in Password Change Interval. Two is the default.

Step 5 Click **Save** to save your security settings.

Note For information about creating login messages, see Creating Messages of the Day, page 6-25.

Manually Disabling Users and Passwords

As described in the Editing User Security Settings, page 6-21, 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 Managing Users and User Security, page 6-15 for more details.

To disable Prime Performance Manager users and passwords:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging In as the Root User, page 2-1.

Step 2 Enter:

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

Step 3 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 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. This also applies to authentication performed by Prime Central single signon.

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

Step 5 To disable a user 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.

Step 6 To re-enable the user account:

- Using the same password—Enter the **ppm enableuser** command.
- Using a new password—Enter the **ppm userpass** command.

Enabling User Accounts and Passwords Using the CLI

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 gateway as the root user. See Logging In as the Root User, page 2-1.

Step 2 Enter the following command:

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

Step 3 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 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 Modifying the Password Policy, page 6-9.

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 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 Modifying the Password Policy, page 6-9.

Step 6 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.

Creating Messages of the Day

You can provision Prime Performance Manager to display a user-defined system message of the day to appear before and after users log in. User s must accept the message before they are allowed to proceed. You can use the message of the day to communicate important system changes or events to users.

To display the message of the day, launch Prime Performance Manager. If a pre-login message of the day is enabled, it is displayed and requires you to accept the message before the login window is displayed. If a post-login message is enabled, it appears right after you log in and requires you to accept it before the Prime Performance Manager window is displayed.

To create or edit the message of the day:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security**

Step 3 On the Users screen, click **Security Settings**.

Step 4 Complete one or both of the following messages:

- To create a pre-login message, check the Pre-Login Message box, enter the message, then click **Save**.
- To create a post-login message, check the Post-Login Message box, enter the message, then click **Save**.

The messages will appear at the next user login.

Note Messages of the day can also be configured using the ppm motd and ppm premotd commands. For information, see ppm motd, page B-60 and ppm premotd, page B-71.

Sending Announcements to Online Users

Administrator users can send announcement messages to all online Prime Performance Manager users. Announcements are displayed in a message window and require users to acknowledge to close the window.

To send an announcement to online users:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the menu bar at the top right window corner, choose **Send Announcement**, shown in Figure 6-1.

Note The Send Announcement tool is only displayed to Administrator users.

Figure 6-1 Send Announcement Tool

Step 3 In the Send an Announcement to All Online Users window, type the message you want to send.

Note If user access is enabled, the message window contains a From field populated with your username.

Step 4 When finished, click **Send Announcement**.

The announcement appears in a popup window on the screens of all online users, Users must click **OK** to dismiss the message.

Displaying Active Sessions

To see a list of users who are actively logged into the server:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Tenants/Security.**

Step 3 On the Users screen, click **Active Sessions**.

Step 4 On the Active Sessions as of [current date] screen, the following user information is displayed:

- Session ID
- Username
- IP/Host Name
- Login Time
- Last Access Time
- Login Method

Listing Currently Defined Users

To list all currently defined users in Prime Performance Manager user-based access account list using the CLI:

Note You can also view user account information on Prime Performance Manager User Management page, see Managing Users and User Security, page 6-15 for more details.

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging In as the Root User, page 2-1.

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
- Password Aging—Whether password aging is enabled for the user.

To list information for a specific user, enter:

```
./ppm listusers username
```

where *username* is the name of the user.

Displaying the System Security Log

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

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging In as the Root User, page 2-1.

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
- 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.

You can also view the system security log on Prime Performance Manager System Security Log web page. For more information, see Displaying the Security Audit Log, page 12-6.