CHAPTER 6

Setting Up and Managing Users

Before you set up your gateway 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.

The following topics provide information about configuring Prime Performance Manager setting up and managing users:

Setting 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 into the system to access the:

- Prime Performance Manager web interface
- Event Editor

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 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, enter:

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

- For Solaris, Prime Performance Manager has both 32-bit and 64-bit JVM versions. 64-bit JVM is enabled by default. To change to 32-bit, enter:

  ```
  % 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 the JVM version, enter:

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

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

  You need to ensure that the proper PAM library version 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 6-6.

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 6-5.
- 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 gateway as the root user. See Logging in as the Root User, page 2-1.

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

- SSL must be enabled. See Enabling SSL on Gateways and Units, page 5-1.
- 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 B, "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 gateway using the **/opt/CSCOppm-gw/bin/ppm restart** command (see ppm restart, page B-39).

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

See Creating Secure Passwords, page 6-5, 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 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:

  – 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:

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 6-2, or **ppm updateuser** or **ppm newlevel** commands, as described in Enabling and Changing Users and Passwords, page 6-10.

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 the 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 (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 ten 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 6-7, 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 Managing Prime Performance Manager Users, page 6-14 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 (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 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 (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 6-5.

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 6-5.

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

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 Managing Prime Performance Manager Users, page 6-14 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

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 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, 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 12-11.

Disabling Prime Performance Manager User-Based Access

To completely disable Prime Performance Manager User-Based Access:

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).

Managing Prime Performance Manager Users

Prime Performance Manager allows you to manage users through the web interface. User access must be enabled. A Level 5 user must be created during installation or post-installation, using Prime Performance Manager CLI as root.

A web user with user management permissions with Prime Performance Manager access Level 5, can add or delete users and modify user passwords and roles/access levels.

To manage users, click **Administrative** in the navigation tree and then click **User Management**. All Prime Performance Manager users are displayed with the time of their most recent logins, their access levels, and their account statuses. Table 6-1 lists the User Management tab information and options.

Table 6-1 User Management Tab

Option	Tool	Description
Create a new user account		Creates a new user account.
Delete an existing user account		Deletes one or more users. The user interface asks for confirmation and deletes the user. To delete multiple users, check the check box in the user row and then click the **Delete an existing user account** button in the toolbar.
Users selected		The number of currently selected users.
Clear Selection		Deselects the selected list of users.

To add a new user:

Step 1 Click **Administrative** in the navigation tree and then click **User Management.**

Step 2 In the User Management window, click the **Create a New User Account** tool.

Step 3 Complete the new user information. The options that appear depend on whether you enabled local authentication or rely on Solaris or Linux user authentication.

- Name—Enter the user name.
- Level—Enter the user authentication level for the user. The valid values are:
  - Basic User, Level 1
  - Network Operator, Level 3
  - System Administrator, Level 5
  - Custom Level 1
  - Custom Level 2
- Password (local authentication only)—Enter the user password.
- Confirm Password (local authentication only)—Retype the password to confirm the new password.
- 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.
- Add users not known to system? (Solaris or Unix authentication only)—If selected, allows users who are not known to the system to be added.

Step 4 Click **OK**.

After you add users, the User Management table contains the following information:

Action—Allows you to change the user's password.

- User—The Prime Performance Manager user for whom a user-based access account is set up.
- Last Login—The date and time the user last logged into Prime Performance Manager.
- Access Level—Authentication level and number for the user. Valid access levels and numbers include:
  - Basic User, Level 1
  - Network Operator, Level 3
  - System Administrator, Level 5
  - Custom Level 1, 11
  - Custom Level 2, 12
- Account Status—The current user's account status: Enabled (the account is functioning normally), or Disabled. A user account can be disabled for the following reasons:
  - A System Administrator disabled the account. See the "ppm disablepass" section on page B-17 and the "ppm disableuser" section on page B-17 for more information.
  - Prime Performance Manager disabled the account because of too many failed attempts to log in using the account. See the "ppm badlogindisable" section on page B-11 for more information.
  - Prime Performance Manager disabled the account because it was inactive for too many days. See the "ppm inactiveuserdays" section on page B-24 for more information.

- Expired Password
- Temporary Password

To update a user:

Step 1 Click the **Change a User's Password** icon under the Action column.

Step 2 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 3 Click **OK**.