CHAPTER 5

Configuring User Access for the Cisco PAM Desktop Client

This chapter describes how to configure operators for the Cisco PAM desktop client.

Note Whenever you upgrade the server software, you must also upgrade the desktop software. If the versions are not the same, an error will occur when launching the desktop client. See Installing or Updating the Cisco PAM Desktop Software, page 4-2.

Contents

Defining User Profiles for Desktop Application Access

Profiles are pre-defined sets of access privileges that define the Cisco PAM modules and commands available to a user. For example, users that should have all privileges can be assigned to the Administrators profile.

If the profile enhancement feature is set in the system configuration settings (for more information, see Data Entry/Validation - Login, page 17-10), the following changes are impacted in this module:

- While creating user profiles, the application prompts the user to select hierarchical location for a specific user profile.
- When the profile enhancement feature is set, the administrator profile cannot be reused even by the cpamadmin, i.e the cpamadmin cannot assign the administrator profile to any profile users.

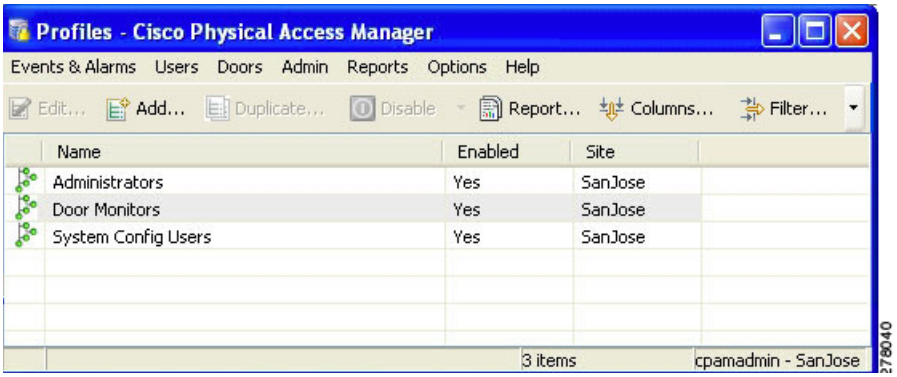
- Assigning a location to a profile in the **Hierarchical location** field specifies the location of the profile. Other than the cpamadmin this specific profile can be accessed only by the users belonging to this location

Note You cannot modify the Administrators profile (read-only).

To create profiles, do the following:

Step 1 Select **Profiles** from the Users menu.

Figure 5-1 Profiles Module Main Page



Step 2 To add a profile, choose **Add**.

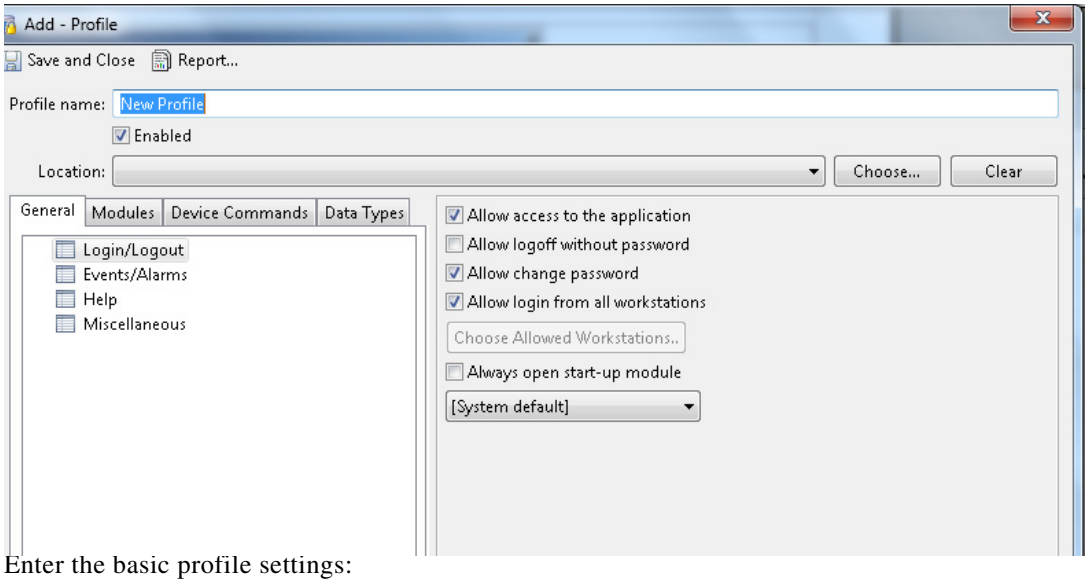
Step 3 Select any one of the following Profile template that closely matches the desired level of user access:

- Default— A basic set of privileges is set.
- Most Restrictive— No privileges are set.
- Least Restrictive— All privileges are set

Figure 5-2 Profile Templates

Step 4 Click **OK** to open the Add Profile screen,

Figure 5-3 Add Profile



Step 5 Enter the basic profile settings:

- Profile name
- Enabled
- Location
- Site(Auto-populated)

Step 6 Click the **General** tab to define the basic profile properties. Check the relevant check boxes next to each field to enable or disable the privilege, as described in Table 5-1.

Table 5-1 General Settings: Profile Module

Field	*Description*
Login/Logout	
Allow access to the application	Allows users to access the application.
Allow logoff without password	Allows users to logoff without the password.
Allow change password	Allows users to change password.
Allow login from all workstations	Allows users to log in to the application from different work stations.
Events/Alarms: Alarm Annotations (Ack., Clear, Comment)	
Allow annotations	Allows users to acknowledge, clear, and comment alarms. Click the **Filter** button to define the events that trigger the action.
Allow multiple annotations	Allows users to acknowledge, clear, and comment multiple alarms at one time.
Allow clearing of unacknowledged alarms	Allows users to clear unacknowledged alarms from the active devices.
Allow clearing of active device alarms	Allows users to clear alarms from active devices.

Table 5-1 General Settings: Profile Module (continued)

Field	*Description*
Require comment on clearing alarms	Allows users to clear the alarms that are not required anymore.
Events/Alarms: On new alarms	
Open Alarms Module	Automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Open Manage Alarm window	Opens automatically to acknowledge/comment/clear the alarms. Click the **Filter** button to define the events that trigger the action.
Open map	Automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show recorded video	Displays recorded video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show live video	Displays live video with new system alarms. Click the **Filter** button to define the events that trigger the action.
Show camera grid	Allows the user to view the video stream in a grid format.
Help: defines access to the different help systems.	
Allow access to help documentation	Allows users to access help documentation.
Enable context menu in help browser	Allows users to view the help context menu.
Allow access to help PDF	Allows users to access the help PDF. To access the helpPDF, Adobe PDF is required.
Miscellaneous	
Allow issuing device command as default	Allows users to issue device commands directly to hardware.
Allow access to external hyperlinks	Allows users to access external hyperlinks.
Require device commands to be commented	Requires users to enter a comment with each device command issued in the system.
Allow editing from right-click menus	Allows users to access the right-click Edit menu.
Allow edit preferences	Allows users to edit preferences.
Rich client: Open modules in new window	Allows users to open modules in a new window.

Step 7 Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 5-5.

a. Select a Cisco PAM module.

b. Select **Allow access to module** to enable access to the module.

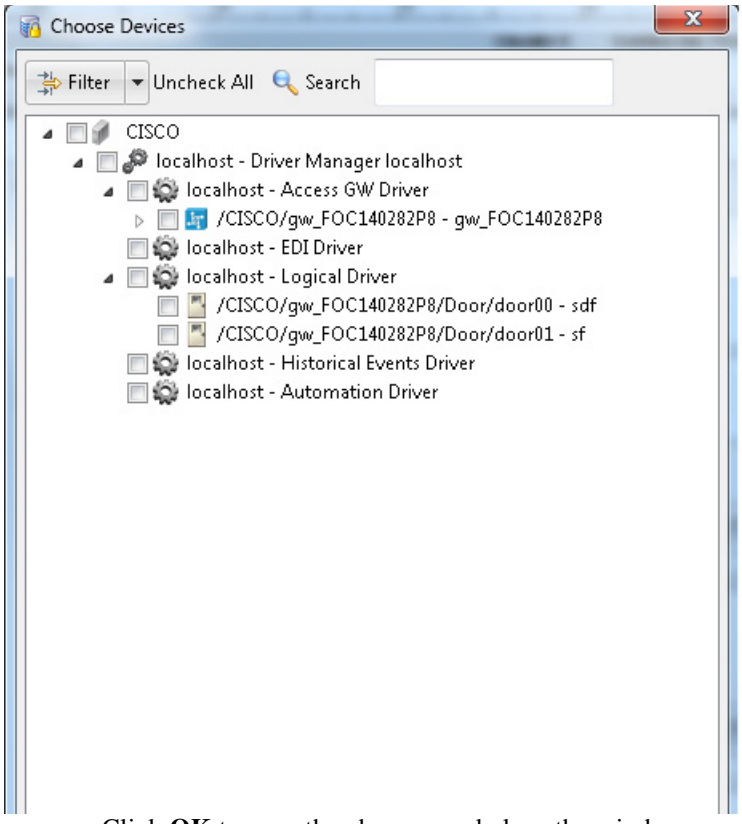
c. (Optional) Use the **Default Filter** with modules such as Event, Badge, and Personnel to define the filter applied when a user opens the module.

Example

To create a profile with access to the Events module that display events for a specific door by default, complete the following sample steps:

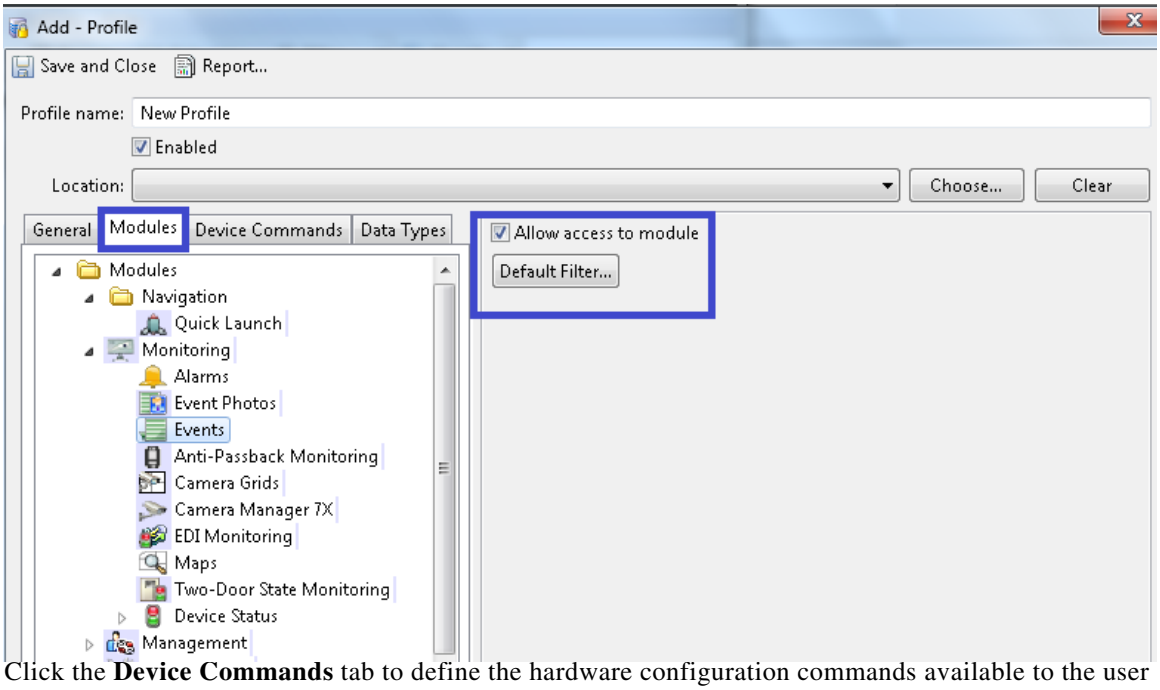
- Create a profile with access to the Events module, as described in the previous steps.
- Click **Default Filter**, as shown in Figure 5-5.
- Select the **Device** tab.
- Click **Choose**.
- In the Choose Devices window, expand the Logical Driver device tree and select a door.

Figure 5-4 Choose Device



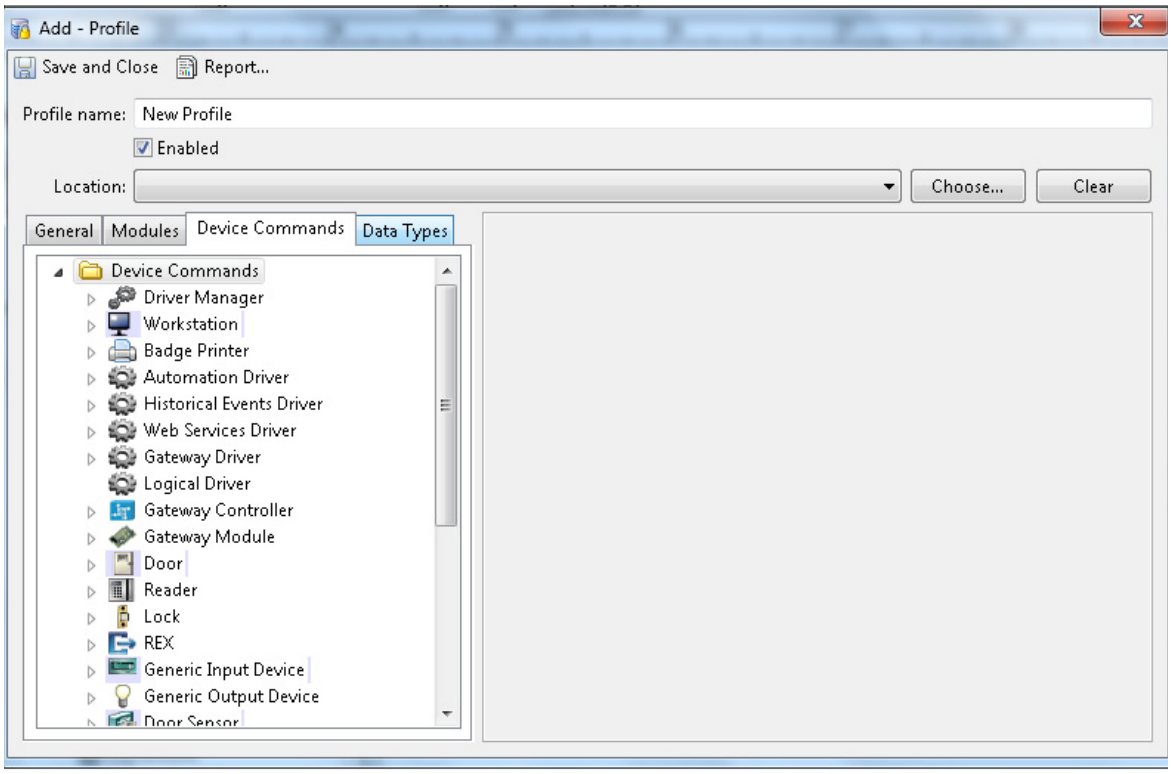
- Click **OK** to save the changes and close the windows.

Figure 5-5 Profile-Modules Tab



Step 8 Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-6).

Figure 5-6 Profiles- Device Command Tab



a. Expand or collapse the list of commands for a device.

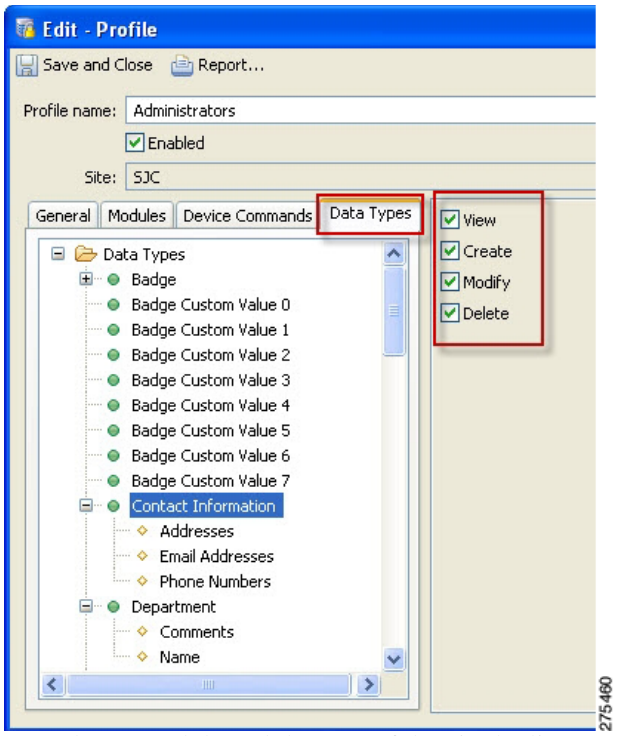
b. Highlight a command.

c. Select the following options:

- **Allow Command to be issued:**
  - **Default**: If user has access to issue device commands, the command access is enabled by default.
  - **No**: Deny access to the command.
  - **Yes**: Allow access to the command.
- **Filter**: Apply a filter to limit the devices for the command.

Step 9 Click the **Data Types** tab to define the data available to the profile.

Figure 5-7 Profiles-Data Type



a. Select a module and the type of data in the list.

b. To restrict the data, check the check boxes for the following properties:

Table 5-2 Profile: Data Types

Field	Description
View	Allows the user to view the selected data type.
Create	Allows the user to add and create the selected data types.
Modify	Allows the user to modify existing data.
Delete	Allows the user to delete data.

Step 10 Click **Save and Close** to save the profile settings.

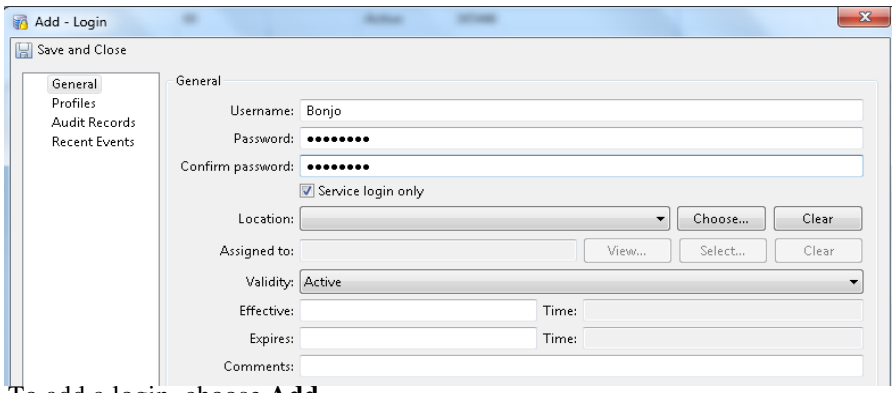
Step 11 Assign the profile to one or more Cisco PAM operators using the **Logins** module. See Creating User Login Accounts and Assigning Profiles.

Creating User Login Accounts and Assigning Profiles

To give users access to Cisco PAM functionality, create a login account and assign one or more access profiles to the username.

Step 1 Select **Logins** from the Users menu. The main window (Figure 5-8) lists all the usernames in the system.

Figure 5-8 Logins Module Main Window



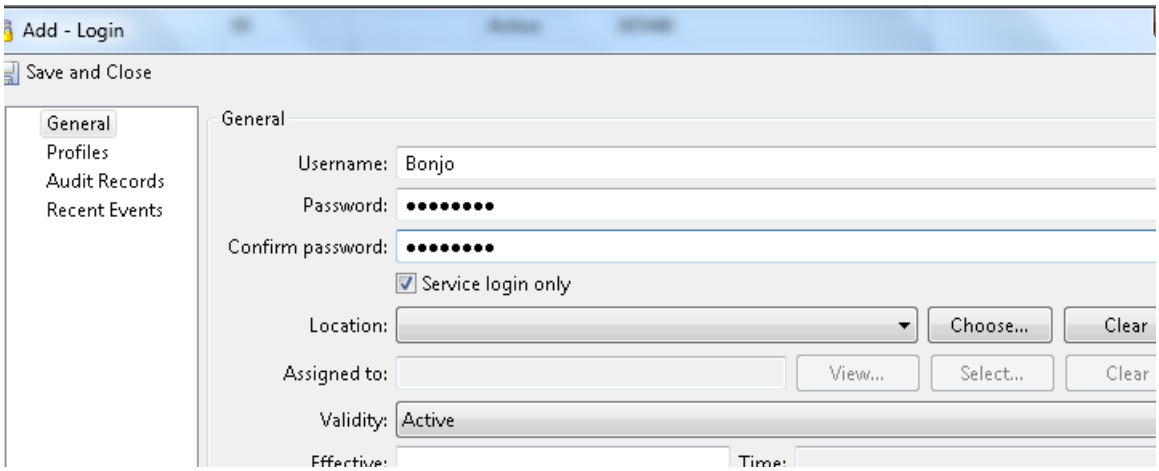
Step 2 To add a login, choose **Add**.

- To modify an existing login, select the entry and choose **Edit**.
- To remove a login, select the entry and choose **Delete**.

Note You cannot modify most of the properties of the **cpamadmin** login.

Step 3 Complete fields in the General tab, Table 5-3 describes the field properties.

Figure 5-9 Logins Module: General Tab



Note The **Username**, **Password**, and **Confirm password** fields are required.

Table 5-3 General Tab Fields.

Field	Description
Username	Required. The username of the login.
Password	Required. Password to access the system.

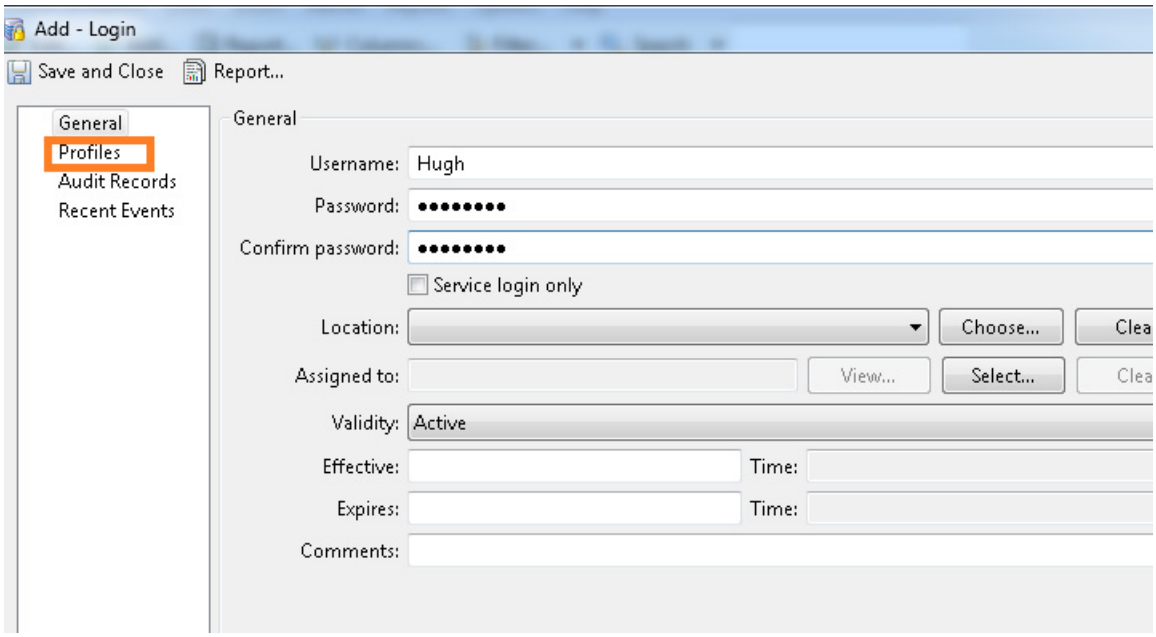
Table 5-3 General Tab Fields. (continued)

Field	Description
Confirm password	Required. The value must be entered exactly as it was in the **Password** field.
Location	This field specifies the login location of a user. Each login location can be accessed only by users belonging to that specific location.
Assigned to	The personnel record the login is assigned to. If the login is for an operator already entered in the **Personnel** module, click the **Select...** button. For more information on adding personnel to the system, see Chapter 9, "Configuring Personnel and Badges".
Validity	**Active** or **Inactive**. Only active accounts can access the system.
Effective	The beginning date the user can log in. If left blank, the user can log in immediately.
Time	The login time of the user.
Expires	The day the login expires and access is denied. If left blank, access is allowed indefinitely.
Time	The time the user login expires.
Site	Read-only. A site is a single instance of a Cisco PAM database.
Comments	Comments or notes about the login.

Step 4 To create a location-restricted user:

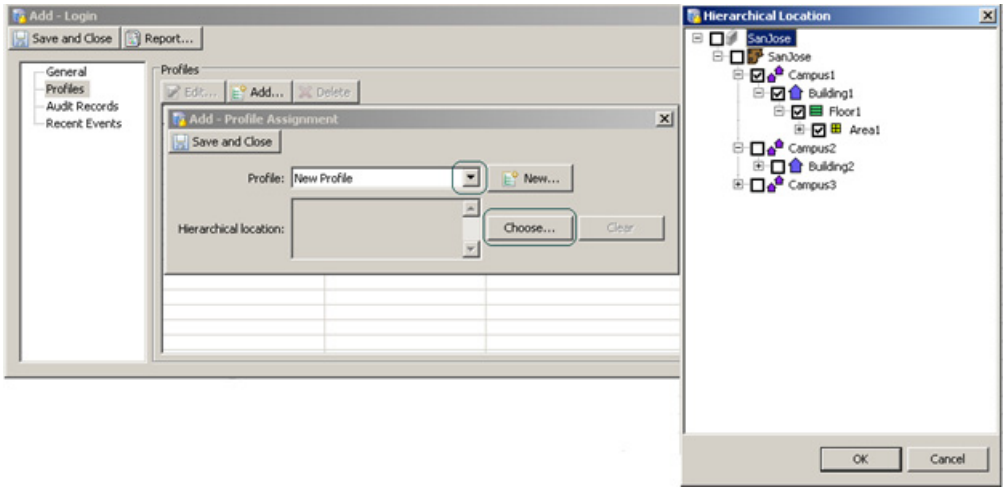
a. Select the **Profiles** tab.

Figure 5-10 Profiles



b. Click **Add**. A new page opens.

Figure 5-11 Add Profile



c. Select an existing **Profile** from the drop-down list or click **New** to create a new profile.

d. Click **Choose** to associate the profile to a specific location in the location hierarchy.

e. Click **Save and Close** to save the changes and close the page.

Step 5 To verify the changes, log off and then log in with the new username and password. Verify whether the appropriate devices are populated for this location-restricted user.

Additional Information

- If the user does not associate a profile to login, the user will not be able to login into the system.
- When a login is associated with a profile without any location, the user associated with that profile is not bound to any hierarchical location and can access devices from all locations.
- Existing logins that have the administrator profile will continue to have the privileges of the administrator. It is the responsibility of the cpamadmin to unassign the administrator profile from these logins if required.

Note If the user does not select the fields that associate locations to logins (See Data Entry/Validation - Login, page 17-10), the user actions are not restricted to the locations. The configuration settings now reflects the Cisco Physical Access Manager 1.3 release.

Configuring LDAP User Authentication

To authenticate users using a Lightweight Directory Access Protocol (LDAP) server, do the following:

- Configure the LDAP Server, page 5-12
- Create the LDAP User Account in Cisco PAM, page 5-14

Configure the LDAP Server

Enter the LDAP server settings to configure the LDAP server connection and user authentication, as described in the following instructions.

Step 1 Select **System Configuration** from the Admin menu, and then select the **LDAP** tab.

Step 2 Enter the LDAP user authentication settings. The LDAP configuration depends on the authentication mode:

- **User principal name** (recommended method). The user principal name is unique in the organization.
- **sAMAccountName**: the samaccount username is unique only in the search domain.

LDAP uses a principle to authenticate. The principle is formed from the username: prefix + username + suffix. The exact format of the principle varies based on the type of LDAP server, and the domain.

For OpenLDAP, the prefix should be: uid=
The suffix should be changed to reflect the actual domain.
So for my-domain.com, this would be:
,dc=my-domain,dc=com

For more information, see the following:

- LDAP Example: User Principal Name, page 5-13
- LDAP Example: sAMAccountName, page 5-14

Step 3 Enter the other LDAP server settings (Table 5-4):

Table 5-4 LDAP System Configuration Settings

Field	Description
Enable LDAP	Click the check box to enable or disable LDAP support.
LDAP server URL	URL of LDAP server, must begin with `ldap://` Example: `ldap://192.168.1.1:389` **Note** 389 is the port number.
Principle suffix	Appended to the username for authentication. See above.
Principle prefix	Prepended to the username for authentication. See above.

Table 5-4 LDAP System Configuration Settings (continued)

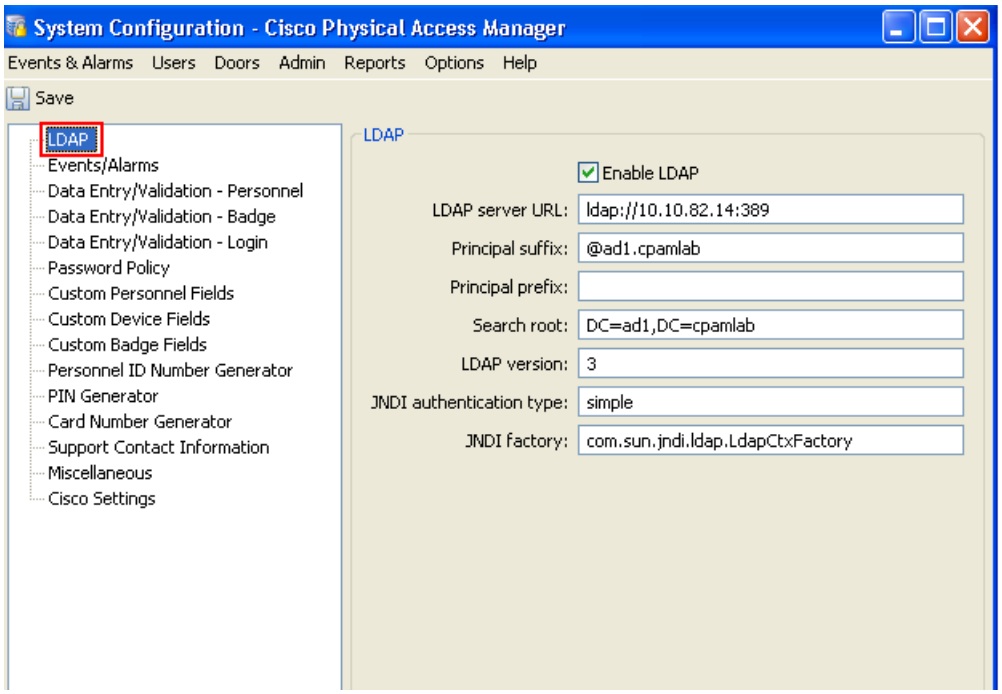
Field	Description
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: `cn=Users,dc=my-domain,dc=com`. • For OpenLDAP, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com:`dc=my-domain,dc=com`.
LDAP version	An advanced setting that generally should be left unchanged.
JNDI authentication type	An advanced setting that generally should be left unchanged as `simple`.
JNDI factory	An advanced setting that generally should be left unchanged as `com.sun.jndi.ldap.LdapCtxFactory`

Step 4 Stop and start the Cisco PAM application from the web admin page to enable the changes.

LDAP Example: User Principal Name

In the example shown in Figure 5-12, the user principal name is `cpsm.user@ad1.cpamlab`. The Cisco PAM user login must be the same (`cpsm.user`).

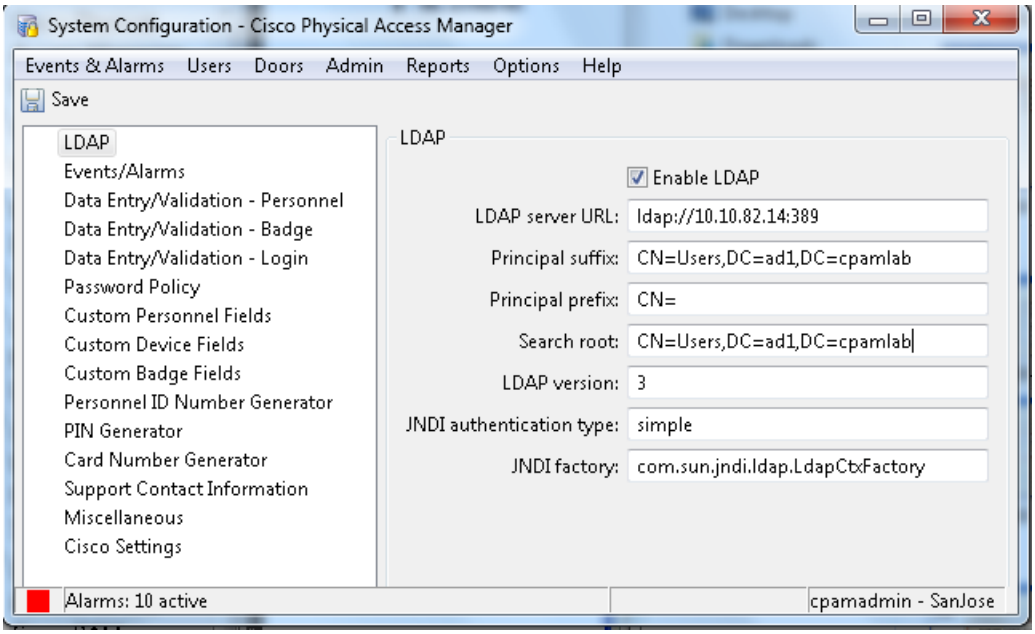
Figure 5-12 User Principal LDAP Configuration Example



LDAP Example: sAMAccountName

In the example shown in Figure 5-13, the user login is the same as the samaccount name (`cpsmuser`).

Figure 5-13 sAMAccountName: LDAP Configuration Example

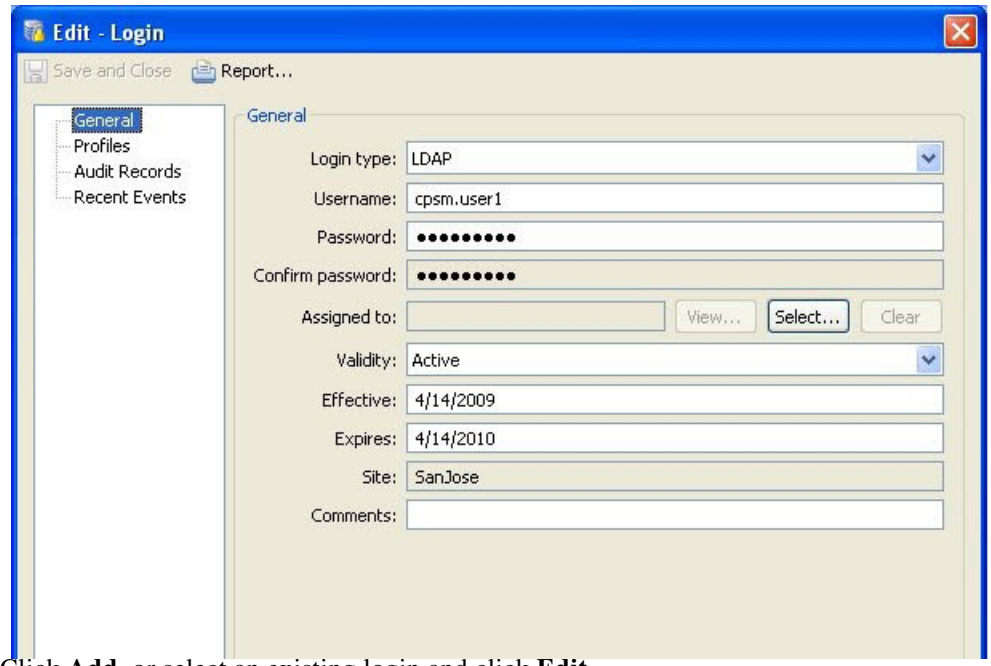


Create the LDAP User Account in Cisco PAM

Create the user account to be authenticated using an LDAP server:

Step 1 Select **Logins** from the Users menu.

Figure 5-14 Login Window: LDAP Login Type



Step 2 Click **Add**, or select an existing login and click **Edit**.

Step 3 Select the Login type **LDAP**. The Login type field appears only if LDAP was enabled and the Cisco PAM application was restarted (see Configure the LDAP Server, page 5-12).

Step 4 Enter the username, password, and other settings for the LDAP login. See Creating User Login Accounts and Assigning Profiles, page 5-8.

Note Although a password must be entered for all user Login records, it is not used for LDAP authentication. LDAP servers use the password entered when the user logs in to Cisco PAM.

Step 5 Click **Profiles** and select the user's Cisco PAM profiles. See , page 5-1 for more information.

Note Cisco PAM does not synchronize the LDAP profiles.

Step 6 Click **Save and Close**.

Viewing Audit Records for Changes to Usernames

An audit record is generated every time a user adds, deletes, or modifies a Login entry. To view the audit record:

Step 1 Select **Logins** from the User menu.

Step 2 Double-click a username entry (or select the entry and click **Edit**).

Step 3 Select **Audit Records**, as shown in Figure 5-15.

Step 4 Double-click an entry to view details for the item. Table 5-5 describes the audit record fields.

Figure 5-15 Logins Audit Records Window

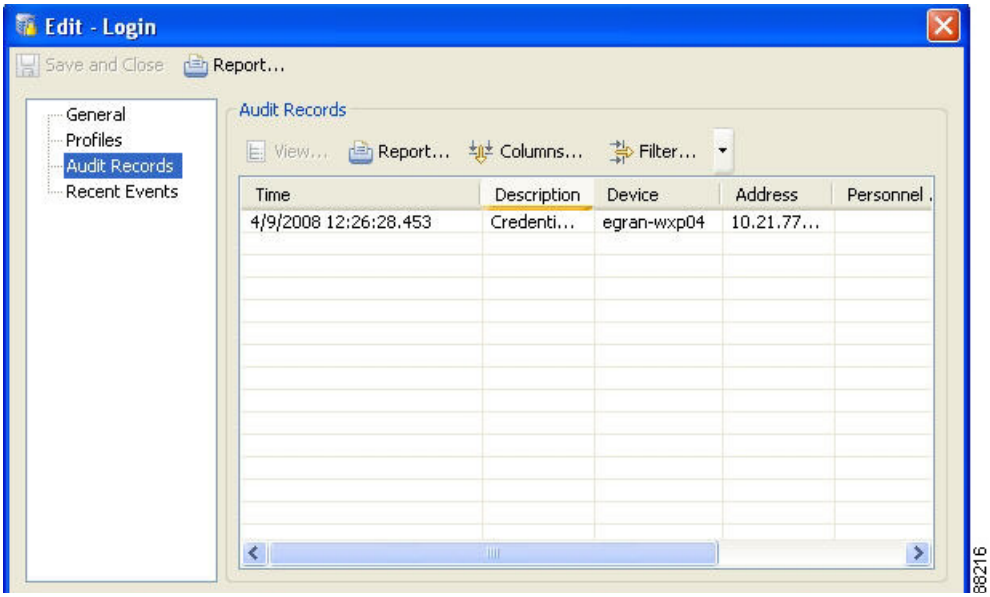


Table 5-5 Logins Module: Audit Records Fields

Field	Description
Time	The time and date when the modification occurred.
Time Received	The time and date when the modification was saved.
Site	The site where the modification occurred. A site is a single instance of a Cisco PAM database.
Type	The type of change.
Log code	An abbreviated code uniquely identifying the type of change.
Priority	A priority used for sorting events and alarms. Positive priorities are above normal priority, while negative priorities are below normal priority. Zero is normal.
Description	A description of the change.
Device	The workstation name where the modification occurred. Click **View** to display details for the device where the change was made, including the IP address of the workstation device.

Table 5-5 Logins Module: Audit Records Fields (continued)

Field	Description
Credential	The username used when the modification occurred. Click **View** to display and revise details for the username.
Personnel record	The name of the operator associated with the modification (if the login was associated with a personnel record at the time).
Data	Additional information about the modification.
View Current...	Opens a new window displaying the current settings.
View Before...	Opens a new window displaying the settings before the change was made.
View After...	Opens a new window displaying the settings after the change was made.

Managing Desktop Client Passwords

Tip To determine password expiration and strength requirements, see Password Policy Settings, page 17-11.

Changing Your Password

To change the password for the account currently logged in to the system, do the following:

Step 1 From the Options menu, select **Change Password**.

Step 2 Enter your old password, and then enter a new password.

Step 3 Re-enter the new password to confirm the setting.

Step 4 Click **OK**.

Changing Another User's Password

To change another user's password, edit the Login record for that user. See Creating User Login Accounts and Assigning Profiles, page 5-8 for instructions.

Note You must have access privileges for the Login module to change passwords.

Managing the *cpamadmin* Login and Password

The **cpamadmin** login and password are created during the initial server setup, as described in Chapter 3, "Configuring and Monitoring the Cisco PAM Server". After the initial setup, however, the **cpamadmin** login and password for the desktop client are managed independently of the server login: changes to the desktop login do not effect the server login. See Changing or Recovering the Server Password, page 3-39 for more information.

To retrieve a lost password for the **cpamadmin** user on the desktop client, log in with another user's account that has administrator privileges, and then reset the **cpamadmin** user password.