



CHAPTER 7

Administration

Cisco PVM contains simple GUI windows for performing administrative tasks. Two user types are managed under the Admin tab: Administrators and General Users. All users can change their own passwords, while Administrators can also view system and security events, as well as manage access to the system for all users.

This chapter contains the following sections:

- [The Admin GUI, page 7-1](#)
- [User Management, page 7-9](#)
- [Changing the Cisco PVM Password, page 7-15](#)

The Admin GUI



Note

The functions discussed in this section apply to Cisco PVM Administrators only.

Clicking the Admin tab opens the Admin GUI, which defaults to the Security Logs window (see [Figure 7-1.](#))

Figure 7-1 Admin GUI – Default

The screenshot displays the Cisco Performance Visibility Manager Admin GUI. The top navigation bar includes tabs for Setup, Monitor, Reports, ART, Alerts, and Admin. The main content area is titled "Security Logs" and features a table with 13 items. The table columns are Severity, Date, Log Type, Description, and Log Source Type. The log entries include various events such as User Login Success, User Logout, and User Login Failure, with severity levels ranging from Information to Warning.

Severity	Date	Log Type	Description	Log Source Type
Information	01/24/2006 14:20:52	Login	User Login Success	Generic
Information	01/24/2006 14:20:47	Logout	User Logout	Generic
Information	01/24/2006 14:18:31	Login	User Login Success	Generic
Warning	01/24/2006 14:18:24	Login	User Login Failure	Generic
Warning	01/24/2006 14:18:13	Login	User Login Failure	Generic
Information	01/24/2006 14:10:58	Generic	PVM Mode	Cisco PVM
Information	01/24/2006 14:07:54	Login	User Login Success	Generic
Information	01/24/2006 14:04:56	Generic	PVM Mode	Cisco PVM
Warning	01/24/2006 13:59:37	Login	User Login Failure	Generic
Information	01/24/2006 13:59:22	Generic	PVM Mode	Cisco PVM
Warning	01/24/2006 13:58:07	Login	User Login Failure	Generic
Information	01/24/2006 13:57:32	Generic	PVM Mode	Cisco PVM
Information	01/24/2006 13:40:04	Login	User Login Success	Generic

Security Logs

Cisco PVM uses HTTPS to provide secure communication between the browser client and the server components. The security configuration is set in the system and does not require any user intervention or setup. Cisco PVM polls system data for security violations and other events, including:

- Login events
- Logout events
- Login failures
- NAM Traffic Analyzer launch from the Cisco PVM GUI

Administrators can display the logged events under the Admin tab, and can filter events occurring within a specific time period by time period, severity, log type, source, and cause.

This section includes the following topics:

- [Event Severity Color Codes, page 7-2](#)
- [Displaying the Security Logs, page 7-3](#)
- [Filtering the Event List, page 7-6](#)
- [Displaying Security Log Details, page 7-7](#)



Note

The functions discussed in this section apply to Cisco PVM Administrators only.

Event Severity Color Codes

Cisco PVM displays a color-coded icon next to each security event indicating severity. [Table 7-1](#) shows the color assigned to each severity level.

Table 7-1 Event Severity Color Codes

Severity	Color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Cyan
Cleared	Green
Indeterminate	Blue
Information	Gray

Displaying the Security Logs

The default Security Log view for Cisco PVM displays security events that have occurred over the last hour. Administrators can also filter alerts occurring over specific time periods by type, severity, source, and cause.

Step 1 On the Cisco PVM Dashboard, click:

- the **Admin** tab or
- **Security Logs** in the Admin navigation menu.

The Security Logs window is displayed (Figure 7-2), showing the alerts for the last hour.



Tip You can sort the list in ascending or descending order by clicking any of the column headers.

Figure 7-2 Security Logs Window

Security Logs

From Date: 01/24/2006 01:33 PM To Date: 01/24/2006 02:33 PM Log Type: [] Clear

Description: [] Severity: [] Cause: [] Filter

13 items found, displaying all items. 1

Severity	Date	Log Type	Description	Log Source Type
Information	01/24/2006 14:20:52	Login	User Login Success	Generic
Information	01/24/2006 14:20:47	Logout	User Logout	Generic
Information	01/24/2006 14:18:31	Login	User Login Success	Generic
Warning	01/24/2006 14:18:24	Login	User Login Failure	Generic
Warning	01/24/2006 14:18:13	Login	User Login Failure	Generic
Information	01/24/2006 14:10:58	Generic	PVM Mode	Cisco PVM
Information	01/24/2006 14:07:54	Login	User Login Success	Generic
Information	01/24/2006 14:04:56	Generic	PVM Mode	Cisco PVM
Warning	01/24/2006 13:59:37	Login	User Login Failure	Generic
Information	01/24/2006 13:59:22	Generic	PVM Mode	Cisco PVM
Warning	01/24/2006 13:58:07	Login	User Login Failure	Generic
Information	01/24/2006 13:57:32	Generic	PVM Mode	Cisco PVM
Information	01/24/2006 13:40:04	Login	User Login Success	Generic

149810

Table 7-2 describes the fields in the Security Logs window.

Table 7-2 Security Logs Window Field Descriptions

Field	Type	Description
From Date	Field	Displays the starting date and time of the logs in the list, and accepts the date selection from the pop-up calendar.
Calendar	Icon	Displays a pop-up calendar for selection of date and time.
To Date	Field	Displays the ending date and time of the logs in the list, and accepts the date selection from the pop-up calendar.
Log Type	Drop-down list	Allows selection of the type of violation for filtering the list: <ul style="list-style-type: none"> • Generic • Unknown • Login • Logout • NAM Login
Description	Text box	Allows entry text for filtering the list. Note Sample keywords you might use to search the list include “success,” “failure,” “login”, or “NAM.”
Severity	Drop-down list	Allows selection of the severity type for filtering the list: <ul style="list-style-type: none"> • Indeterminate • Critical • Major • Minor • Warning • Cleared • Information
Cause	Drop-down list	Allows selection of the cause of the event for filtering the list: <ul style="list-style-type: none"> • Generic • Unknown
Clear	Button	Clears all of the fields in the filter area for performing a new filter operation.
Filter	Button	Filters the list of events based on one or more criteria entered in the filter area.
Severity	Column header	Lists the severity level next to a color code and links to the Security Log Detail window for individual events.
Date	Column header	Displays the date and time the event occurred.

Table 7-2 Security Logs Window Field Descriptions (continued)

Field	Type	Description
Log Type	Column header	Displays the type of event that created the alert: <ul style="list-style-type: none"> • Generic • Login • Logout • NAM Login • Purge Messages • Archive Messages • Unknown
Description	Column header	Displays the details of the event, such as: <ul style="list-style-type: none"> • User Login Success • User Logout • User Login Failure • PVM Mode
Log Source Type	Column header	Displays the originating source of the type of alert log created for the violation: <ul style="list-style-type: none"> • Generic • Unknown • Cisco PVM • NAM

Filtering the Event List

The Security Logs list can be filtered based on time interval, log type, severity, source, or cause. You can filter the event list using any or all of the fields at the top of the Security Logs window.

- Step 1** Click **Admin** in the Cisco PVM dashboard, or click **Security Logs** from the Admin navigation menu. The Security Logs window displays a paginated list of all of the alerts generated in the last hour, in descending order by date and time.
- Step 2** Select the start date by clicking the calendar icon next to the **From** field.
- Step 3** Select the end date by clicking the calendar icon next to the **To** field.
- Step 4** Select the traffic type from the **Log Type** drop-down list.
- Step 5** Enter a keyword or characters in the **Description** box, using the percent symbol (%) as a wildcard to broaden your search.
- Step 6** Select the severity level from the **Severity** drop-down list.
- Step 7** Select the event cause from the **Cause** drop-down list.

Step 8 Click **Filter**.

The window displays the Security Logs list containing only the alerts that match the filter criteria.



Tip If you want to begin filtering with a new set of criteria, click **Clear** to reset all of the fields in the filter area to blank.

Displaying Security Log Details

Step 1 Click the link in the Severity column of the event you want to view. The Security Log Detail window (Figure 7-3) displays the log's description along with the log type, database information, and additional details indicating why the event was generated in the system.

Figure 7-3 Security Log Detail

Security Log detail	
Log Id:	163
Log Type:	Login
Date:	2006-01-24 14:18:24.0
Severity:	Warning
Login Id:	pvmadm
Account Type:	
Managed Object Id:	
Managed Object Name:	
Description:	User Login Failure
Log Content:	Username==pvmadm Reason==Bad username or password.

149809

Table 7-3 describes the fields in the Security Log Detail window.

Table 7-3 Security Log Detail Field Descriptions

Field	Description
Log Id	The sequential number of the alert as it appears in the database.
Log Type	The type of alert generated: <ul style="list-style-type: none"> • Generic • Login • Logout • NAM Login
Date	The date and time the event occurred.

Table 7-3 Security Log Detail Field Descriptions (continued)

Field	Description
Severity	The severity level of the event: <ul style="list-style-type: none"> • Indeterminate • Critical • Major • Minor • Warning • Cleared • Information
Login Id	The login ID used to attempt access to Cisco PVM or the NAM Traffic Analyzer.
Account Type	The type of user attempting to log in to or log out of the system: <ul style="list-style-type: none"> • Administrator • General User
Managed Object Id	The classification of the managed object as it appears in the database.
Managed Object Name	The name of the managed object as it appears in the database.
Description	The originating event, such as login success or failure.
Log Content	Detailed information about the actual event as contained in the database, such as: <ul style="list-style-type: none"> • the correct login ID as listed in the database. • the actual data that created the event, such as a bad user name or password.

Step 2 Close the Security Log Details window by clicking **Back**.

The system returns to the Security Logs window.

Using the Troubleshooting Utility

Cisco PVM provides a GetPVMInfo utility that gathers information for troubleshooting purposes. The GetPVMInfo utility checks the Cisco PVM installation and environment. These results, along with key Cisco PVM logs and trace files, are collected and consolidated into an archive.

The GetPVMInfo utility is located in the /opt/CSCOpvm/server/bin directory. It can only be executed by the pvmdm user. The results archive is located in the same directory and is named GetPvmInfo_[timestamp].tgz. For example:

```
su - pvmdm
cd opt/CSCOpvm/server/bin
./GetPVMInfo
```

Alternately, you can execute a pvm debug command to launch the GetPVM Info utility. For example:

```
su - pvmdm
pvm debug
```

**Caution**

The Cisco PVM application and database functions require proper configuration of the Linux shell environment. After Cisco PVM installation, a shell environment file is created at `$PVM_BASE/bin/shellrc` and registered as part of the Cisco PVM RPM package (`ciscopvm1-mc_shared`). This file is used by the Cisco PVM application and database processes automatically at Cisco PVM runtime. For Cisco PVM maintenance and troubleshooting with Linux command-line operations, it is highly recommended for the OS administrator or the `pvmadm` user to configure their system/user environment profile to source this shell environment file or its equivalent copy to set the required environment variables. Changing the original copy of the Cisco PVM shell environment file at `$PVM_base/bin/shellrc` without consulting Cisco PVM product documentation or Cisco PVM technical support is not recommended.

User Management

Access to Cisco PVM requires permission-based security assignments set up under the Admin tab by Cisco PVM Administrators. Users are assigned to groups, or Account Types, which are sets of users with identical access permissions available in the GUI. Cisco PVM supports two Account Types, with the following permissions for user management functions in the GUI:

- **Administrator**—permission to list, add, edit, and delete users, assign users to groups, and change user passwords.
- **General User**—permission to change assigned password only.

**Note**

For a summary of access to Cisco PVM GUI functions by user Account Type, see [User Access to Cisco PVM Functions, page 1-3](#).

This section contains the following topics:

- [LDAP Authentication, page 7-9](#)
- [Listing User Accounts, page 7-10](#)
- [Filtering the User List, page 7-11](#)
- [Adding a User Account, page 7-12](#)
- [Editing a Current User, page 7-13](#)
- [Deleting a Current User](#)

**Note**

The topics in this section apply to Cisco PVM Administrators only.

LDAP Authentication

By default, Cisco PVM relies on its own authentication and authorization repository created during installation. After installation, the system can be configured to use an LDAP (Lightweight Directory Access Protocol) server for user authorizations instead of the Cisco PVM repository. If your system has been configured to use LDAP, the following functions are no longer available through the Cisco PVM GUI:

- Viewing the list of Cisco PVM users

- Adding, editing, or deleting users
- Changing user passwords

If the system has been configured to use LDAP authentication, you'll see a message informing you that all user management functions are maintained in an enterprise-specific tool outside of the Cisco PVM system.

If you have already set up users through the Cisco PVM GUI and subsequently decide to implement LDAP, existing users are retained in the Cisco PVM repository, but are not automatically transferred to LDAP. The system configuration can be changed to use either LDAP or Cisco PVM repositories at any time, but the user assignments are always maintained separately. Therefore, a user previously able to access the system using LDAP login information will not be able to access Cisco PVM until he or she has login information set up specifically in the system.

**Note**

To use LDAP authentication, an ACS server is needed.

Listing User Accounts

Step 1 Click **Admin** on the Cisco PVM dashboard.

Step 2 Click **Users** in the navigation menu.

The User Management window displays all users currently set up in the system (see [Figure 7-4](#)).

Figure 7-4 User Management Window

5 items found, displaying all items.	Login ID	Name	Account Type
<input type="checkbox"/>	cnamadm	Cisco PVM Administrator	Administrator
<input type="checkbox"/>	general1	general1	General User
<input type="checkbox"/>	stevegen	Steven Camden	General User
<input type="checkbox"/>	susangen	Susan Smith	General User
<input type="checkbox"/>	virginia	virginia	Administrator

[Table 7-4](#) describes the fields in the User Management window.

Table 7-4 User Management Field Descriptions

Field	Type	Description
Login ID	Text box	Allows text entry of the user login ID for filtering the list.
Name	Text box	Allows text entry of the user name for filtering the list.
Account Type	Drop-down list	Displays a list of user Account Types for filtering the list: <ul style="list-style-type: none"> • Administrator • General User
Clear	Button	Clears all of the fields in the filter area for a new search operation.
Filter	Button	Returns a list of users matching the filtering criteria.
Login ID	Column Header	Displays the login ID of each user next to a checkbox that allows selection of individual users for viewing, editing, or deletion.
Name	Column Header	The name of the user assigned to the login ID.
Account Type	Column	Displays the type assigned to each user: <ul style="list-style-type: none"> • Administrator • General User
Add	Button	Opens the Add New User window for addition of new users to the system.
Edit	Button	Opens the Edit User window for editing of users currently in the system. Note This button is dimmed until a single user is selected from the list.
Delete	Button	Deletes selected users from the list and the system. Note This button is dimmed until at least one user is selected from the list.

Filtering the User List

You can filter the User Management list based on any or all of the criteria in the filter area. Clicking **Filter** without entering any criteria will return a list of all users in the system.

-
- Step 1** Click **Users** on the Admin navigation menu.
- The User Management list appears, showing all users currently in the system.
- Step 2** Enter a login ID or keyword in the **Login ID** field, using: the percent symbol (%) as a wildcard to broaden your search.
- Step 3** Select the user type from the **Account Type** drop-down list: Administrator or General User.
- Step 4** Enter a user name or keyword in the **Name** field, using: the percent symbol (%) as a wildcard to broaden your search.
- Step 5** Click **Filter**.
- The User Management window displays the list of users matching the filter criteria.



Note To clear the filter criteria and begin a new search, click **Clear**.

Adding a User Account

User accounts can be added to Cisco PVM by Administrators. Required information for new users includes:

- Login ID
- Username
- Password
- Account Type

Step 1 Click **Admin** on the Cisco PVM dashboard. The Security Logs window appears.

Step 2 Click **Users** in the navigation menu.

The User Management window displays a paginated list of all users currently in the system.

Step 3 Click **Add**. The Add New User window appears (see [Figure 7-5](#)).

Figure 7-5 User Management - Add New User

[Table 7-5](#) describes the fields in the Add New User window.

Table 7-5 Add New User Field Descriptions

Field	Type	Description
Login ID	Text box	Text entry of a unique login ID. Note The login ID must be unique or the system will reject creation of the new user.
Name	Text box	Text entry of the user's actual name.
Password	Text box	Encrypted entry of the new user's password, from 1 – 29 characters.
Confirm Password	Text box	Encrypted re-entry of the text entered in the Password field. Note The Confirm Password entry must match the Password entry or the system will reject creation of the new user.

Table 7-5 Add New User Field Descriptions (continued)

Field	Type	Description
Account Type	Drop-down list	Selection of the user group to which the new user belongs: <ul style="list-style-type: none"> Administrator [default] General User <p>Note If you want to add a specific individual to the system as both an Administrator and a General User, the Login IDs must be different for each Account Type.</p>
OK	Button	Checks the window entries for errors and saves the new user to the system.
Reset	Button	Clears all entries on the Add New User window, and resets the Account Type field to Administrator.
Cancel	Button	Exits the Add New User window without saving changes to the system.

- Step 4** Enter the new user's:
- Login ID—must be unique
 - Name—the only field not required on the Add New User window
 - Password—use 1 to 29 characters
 - Confirmed Password—must match the Password entry
 - Account Type - defaults to the type selected in the last set of filter criteria (if any), otherwise defaults to General User

- Step 5** Click **OK**.

The User Management window displays the list of users matching the last set of filter criteria, and the message “User [login ID] was added” is displayed.



Note If system validation of the new account fails, an error message describing the problem is displayed. If this occurs, fix the problem listed in the message and click OK.

- Step 6** Verify that the new user is in the system by entering the new user's Login ID on the User Management window and clicking **Filter**, or by clicking **Clear Form > Filter** to display the list of all users in the system and paginating through the list.

Editing a Current User

Cisco PVM Administrators can use the User Management GUI to edit users currently in the system. For example, the Administrator may want to change a user type from General User to Administrator. The current user's account type can be edited and saved to the Cisco PVM user base.



Note After changes have been saved to the system, new group permissions and passwords will take effect for subsequent login sessions. Existing login sessions for the edited user (if any) are not affected.

- Step 1** Click **Setup** on the Cisco PVM dashboard.

Step 2 Click **Users** in the navigation menu.

The User Management window displays all users currently in the system.

Step 3 Filter the User Management list to locate the user you want to edit.

- a. Select the Account Type from the drop-down list (Administrator or General User).
- b. Enter keywords in either the Login ID or Name fields, or both.
- c. Click **Filter**.

The list of users matching the filter criteria is displayed.

Step 4 Select the checkbox next the name of the user you want to edit.

The Edit button is enabled; if more than one user is selected, the Edit button becomes dimmed.

Step 5 Click **Edit**. The Edit User window is displayed (see [Figure 7-6](#)).



Note The Login field is unavailable for editing.

Figure 7-6 Edit User

Step 6 Edit one or more of the desired field(s) in the Edit User pane, including:

- Name
- New Password
- Confirm Password
- Account Type



Note If an entry is made in the New Password field, the Confirm Password field must match the new entry, and the new password must be different from the old password.

Step 7 Click **OK**.

The User Management window appears with the list of users matching the last set of filter criteria and the message “User [login ID] was updated.”



Note If system validation of the changes fails, an error message describing the problem is displayed. If this happens, fix the problem described and click **OK**.

Deleting a Current User

Cisco PVM Administrators can use the User Management GUI to delete users currently in the system. Multiple users can be deleted in a single step.

-
- Step 1** Click **Setup** on the Cisco PVM dashboard.
- Step 2** Click **Users** in the navigation menu.
- The User Management window displays all users currently in the system.
- Step 3** Find the user you want to delete:
- Select the User Type from the drop-down list (Administrator or General User).
 - Enter keywords in either the Login ID or Name fields, or both.
 - Click **Filter**.

The list of users matching the filter criteria is displayed.

- Step 4** Select the check box next the name of each user you want to delete.
- The Delete button is enabled.
- Step 5** Click **Delete**. The system prompts you to confirm the deletion.
- Step 6** Click **OK** in the confirmation window to delete the selected users.

The filtered User Management list is displayed with the last set of filter criteria, the selected users deleted, and the message, “The selected user was deleted.”



Note Selecting **Cancel** in the confirmation window returns to the filtered User Management list without deleting any users.

Changing the Cisco PVM Password

All users can change their passwords at any time using the Admin tab. You can enter current, new, and confirmation passwords and save the changes to the system. New password information affects subsequent login sessions only; current user sessions, if any, are unaffected.



Note If the Cisco PVM Administrator has configured the system to use LDAP (Lightweight Directory Access Protocol) user permissions, the change password function is no longer available in Cisco PVM.

- Step 1** Click **Admin** on the Cisco PVM dashboard.
- Step 2** Click **Password** in the navigation menu. The Change Password window ([Figure 7-7](#)) appears with the login ID of the current user dimmed and unavailable for editing in the Login ID field.

Figure 7-7 Change Password Window

Change Password

Login ID:

*Old Password:

*New Password:

*Confirm Password:

* Required field

Ok Cancel

149753

- Step 3** Enter the current password in the Old Password field.
- Step 4** Enter a new password in the Password field, using 1 – 29 characters.
- Step 5** Re-enter the new password in the Confirm field.
- Step 6** Click **OK**.



Note Clicking **Cancel** clears all password fields without saving any changes to the system.

The system saves the new password and displays the message, “Your password was updated” at the top of the Change Password window.



Note If system validation of the changes fails, an error message describing the problem is displayed. If this happens, fix the problem described and click **OK**.