CHAPTER 4

Configuring and Monitoring the Cisco PAM Server

This chapter describes how to configure the Cisco PAM server software, including optional feature licenses and high availability. This chapter also describes the additional server monitoring and configuration features of the Cisco PAM Server Administration utility.

When you log on to the appliance for the first time, a set of initial setup screens appear. Enter the settings and other information as described in this chapter.

After the initial setup is complete, the main administration utility windows are displayed, allowing you to install the Cisco PAM desktop client software and additional feature licenses. A variety of other configuration and monitoring tasks can also be performed.

Contents

About the Cisco PAM Server Administration Utility

The Cisco PAM Server Administration utility is a web-based tool used to enter server settings for the Cisco PAM appliance, including network addresses, feature licenses, and high availability settings. The utility also performs a variety of maintenance and monitoring tasks, including backup and restore, system logs, and resetting the server.

- When you access the utility for the first time, the initial setup screens appear. See Entering the Initial Server Configuration, page 4-4.

- After the initial server configuration is complete, see Performing Additional Configuration, Administration, and Monitoring Tasks, page 4-11.

Note The Cisco PAM server software is different from the desktop client software. The desktop (client) software runs on a PC and is used to configure devices and access control settings.

Logging on to the Cisco PAM Server Administration Utility

To log on to the Cisco PAM Server Administration utility, use one of the following methods:

- Connect a PC directly to the server Eth0 port, as described in Entering the Initial Server Configuration, page 4-4.
- Log in to the Cisco PAM Server Administration utility over the Internet using the Eth0 port IP address. You can also use the Shared IP address when two servers are set up in a redundant HA configuration. Ask your system administrator for the correct IP address.
- The Eth1 port can optionally be enabled for Cisco PAM Server Administration utility connections over the web. The Eth1 port is disabled by default.

Using Redundant Appliances for High Availability

High availability is achieved by installing two Cisco PAM appliances in a redundant configuration. One appliance acts as the active server, and the second runs in warm standby mode. All data and configurations on the active appliance are automatically mirrored on the standby appliance to minimize any data loss or system downtime if a failover occurs. If the active appliance goes off-line, the standby appliance automatically assumes full control of the system, including the Shared IP address and Cisco licences.

Note The high availability (HA) feature requires a separate license. See Obtaining and Installing Optional Feature Licenses, page 4-15.

Understanding IP Addresses on the Cisco PAM Server

IP addresses allow the Cisco PAM hardware and software components to communicate over an IP network. This section describes the different IP addresses used in the system.

Note Contact your system administrator tor for the specific IP address settings used in your system.

Cisco PAM Appliance IP Address

The IP address for the Cisco PAM appliance identifies the server on the IP network and is configured on each Gateway.

- For a standalone Cisco PAM appliance, a single IP address is required on the **Eth0** port.
- For a redundant (HA) server configuration, two IP addresses are required:
  - The **Shared IP Address**: The **Shared IP address** is transferred to the standby server if a failover occurs.
  - The **Eth0** port IP address. The **Eth0** address provides HA communication between the active and standby appliances, and an internet connection for the Cisco PAM Server Administration utility. The active appliance must have a different Eth0 IP address than the standby appliance.

Note The Eth0 IP address is required. The Eth0 port provides communication between the Cisco PAM appliance and the Gateway modules, as well as server to server communication in a redundant (HA) configuration.

Note The Shared IP address and the Eth0 IP address should be on the same subnet. Eth0 and Eth1 can be on separate subnets.

Gateway Module IP Addresses

The Gateway module is configured with the following. See the *Cisco Physical Access Gateway User Guide* for details.

- **Eth0 Configuration** for IP network connectivity with the Cisco PAM appliance.
- **DNS Configuration** if names (not IP addresses) are used for the NTP or CPAM addresses.
- **Cisco PAM Configuration** to define the IP address and port of the Cisco PAM appliance used to manage the Gateway. See Cisco PAM Appliance IP Address.

Entering the Initial Server Configuration

The initial setup screens appear automatically when you boot the Cisco PAM appliance for the first time, (or after a complete system restore). The instructions in this section are for a standalone server, or for the two servers in a redundant (high availability) configuration.

- Before You Begin, page 4-4
- Connecting a PC to the Appliance, page 4-4
- Initial Setup Instructions, page 4-5

Before You Begin

Before you power on the Cisco PAM appliance, you need the following:

- A PC and web browser (Internet Explorer 6.0 and higher, or Mozilla Firefox 2.0 and higher).
- An Ethernet cable to connect your PC directly to the Cisco PAM appliance. Cross-over and straight-through cables are supported.

In addition, gather the following information:

- IP, subnet, and gateway addresses for the Cisco PAM appliance:
  - For a standalone server installation, one IP address for Eth0 is required.
  - For a redundant (HA) server configuration, two IP addresses are required: One address for the Shared IP Address setting, and a second address for the Eth0 port. See Understanding IP Addresses on the Cisco PAM Server, page 4-3.
- (Optional) If using NTP synchronization, the address of the NTP server.
- (Optional) The DNS server settings.
- Administrator password. If you are setting up the appliance for the first time, use the default password supplied in the following instructions.

Connecting a PC to the Appliance

To complete the initial Cisco PAM configuration, connect an Ethernet cable from a PC to the Cisco PAM appliance Eth0 port. Use a web browser to enter the required settings.

Step 1 Connect an Ethernet cable from your PC to the Eth0 port on the Cisco PAM appliance (the Eth1 port is disabled by default). See Appliance Rear Area, page 1-12 for the location of the appliance ports.

Note After configuration is complete, disconnect your the Eth0 cable from the PC, connect the appliance to the IP network.

Step 2 Power on the appliance. See System Front Panel, page 1-11 for the location of the power button.

Step 3 Open a web browser on your PC and enter the URL: https://192.168.1.2.

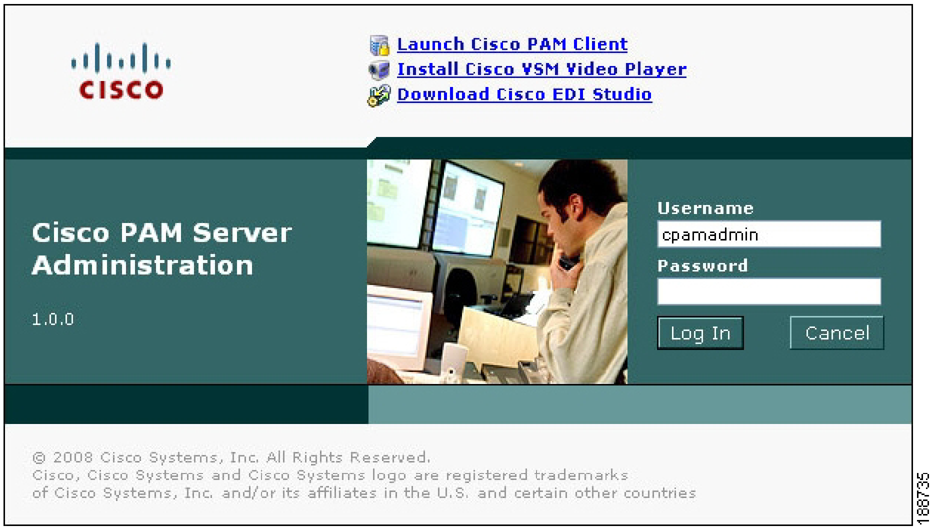
Note Be sure to include the *s* in *https://*. This connects your browser to the secure URL.

Step 4 Enter the default username and password as shown in Figure 4-2:

default username: **`cpamadmin`**

default password: **`cpamadmin`**

Figure 4-1 Cisco PAM Server Administration Utility: Login



Cisco PAM Server Administration

1.0.0

Username: cpamadmin

Password:

© 2008 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

Tip The default password is used the first time you log into the active or standby appliance. You are required to configure a new password during the initial setup, as described in Entering the Initial Server Configuration, page 4-4. Use the new administrator password for subsequent logins, or the username and password supplied by your system administrator. The administrator username cannot be changed.

Initial Setup Instructions

To enter the initial configuration for a Cisco PAM appliance, do the following:

Step 1 Log on to the appliance, as described in Connecting a PC to the Appliance, page 4-4.

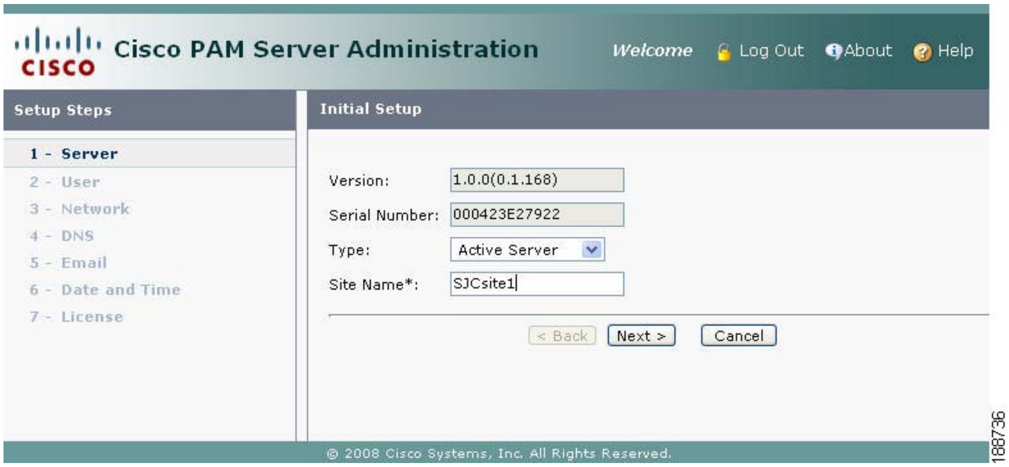
Step 2 Enter the server configuration, as shown in Figure 4-2:

Note The Version and Serial Number are not configurable.

a. **Type**: Select the server type to enable the configuration options for the appliance.

- **Active Server**: (Default) Select **Active Server** for a single appliance, or if the appliance is the active server in a redundant configuration.
- **Standby Server**: Select **Standby Server** if the appliance is the standby (backup) server in a redundant configuration. A standby server must have the exact same configuration settings as the active *except* the network addressees, host name, and HA license.

Figure 4-2 Initial Setup: Server Configuration



Version: 1.0.0(0.1.168)

Serial Number: 000423E27922

Type: Active Server

Site Name*: SJCsite1

b. **Site Name**: Enter a description for the appliance to identify the appliance on the network. This field is disabled for a standby appliance since the standby server assumes the active server name if a failover occurs.

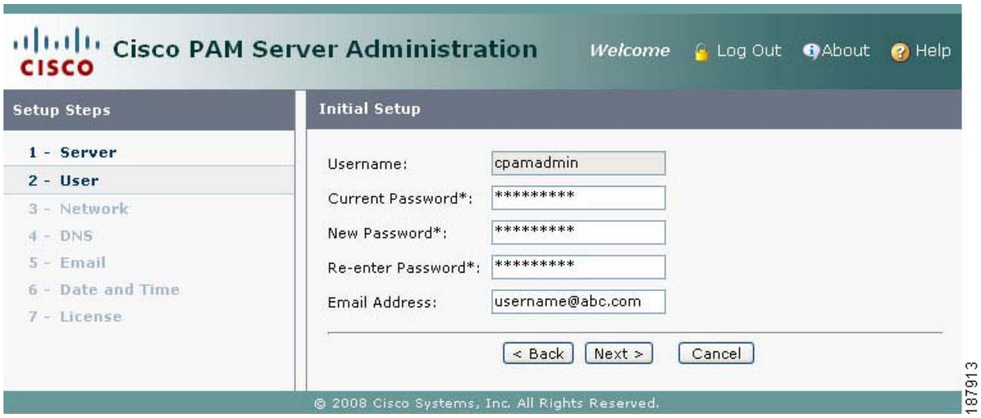
   Enter any combination of letters and numbers up to 32 characters. Spaces are not allowed. Dashes and underscore characters are allowed.

   Example: `SJCSite1`.

c. Select **Next** to apply the settings and continue.

Step 3 Enter the initial User settings to define the administrator password and email address, as shown in Figure 4-3. Enter the same settings on the active and standby appliance.

Figure 4-3 Initial Setup: User Configuration



Username: cpamadmin

Current Password*: *********

New Password*: *********

Re-enter Password*: *********

Email Address: username@abc.com

a. **Username**: The admin username cannot be changed. The default username is **`cpamadmin`**.

b. **Current Password**: Enter the administrator password. The default password is **`cpamadmin`**.

c. **New Password**: Enter a new administrator password. The administrator has full rights to configure the Cisco PAM appliance, and grant access rights to other users. The new password is required and must be entered to continue.

d. **Re-enter Password**: Re-enter the administrator password to confirm the setting.

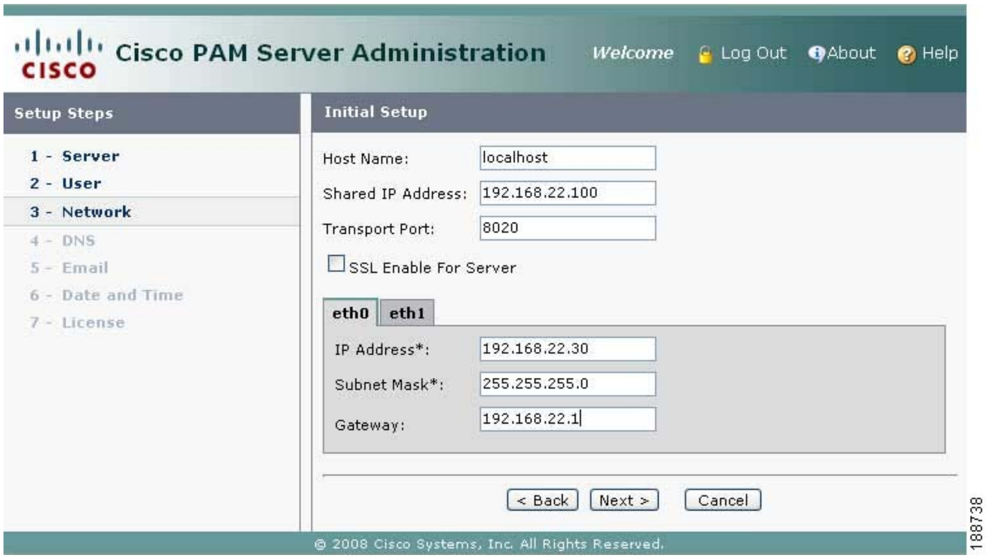
e. **Email Address**: (Optional) Enter the email address that will receive system messages.

f. Select **Next** to apply the settings and continue.

Step 4 Enter the Network configuration for the Cisco PAM appliance, as shown in Figure 4-4.

- The Shared IP address, Port and SSL are the same on the active and standby appliances.
- The host name must be different for the active and standby appliances.
- The Eth0 and Eth1 IP addresses must be different on the active and standby appliances.
- All IP addresses must be on the same subnet.

Figure 4-4 Initial Setup: Network Configuration



Host Name: localhost

Shared IP Address: 192.168.22.100

Transport Port: 8020

☐ SSL Enable For Server

IP Address*: 192.168.22.30

Subnet Mask*: 255.255.255.0

Gateway: 192.168.22.1

Complete the following Network settings:

a. **Host Name**: Enter the host name on the active appliance. Enter a different host name on the standby appliance. The host name is used to identify the appliance on the local network and does not impact other configurations.

b. **Shared IP Address**: (HA configurations only). Enter the same IP address on the active and standby appliance. This address is transferred from the active to the standby appliance if a failover occurs.

The Shared IP address and the Eth0 IP address should be on the same subnet. Eth0 and Eth1 can be on separate subnets. See Understanding IP Addresses on the Cisco PAM Server, page 4-3 for more information.

c. **Transport Port:** The default value is 8020. Enter the same number the same on the active and standby appliances.

d. **SSL Enable For Server**: Click the **SSL** checkbox to enable or disable secure IP communication between the Cisco PAM appliance and the Cisco Physical Access Gateways. The settings must be the same the same on the active and standby appliances.

Note Cisco Systems recommends that SSL always be enabled for all Gateways and the Cisco PAM appliance (default). If SSL is disabled for a Gateway but enabled for Cisco PAM, the Gateway cannot connect to the appliance. If the SSL settings are changed, reset all Gateways and the Cisco PAM appliance.

e. **Eth0**: (Required) Enter a static IP address for the Eth0 port. If the appliance is a standalone server, this port is the Cisco PAM appliance IP address. In a redundant (HA) configuration, the Eth0 port is used for HA communication between the active and standby appliance. The active appliance must have a different Eth0 IP address than the standby appliance.

   See Understanding IP Addresses on the Cisco PAM Server, page 4-3 for more information.

   – **IP Address**: Enter the IP address for the Eth0 port. This address should be on the same subnet as the Shared IP address, and must be different on the active and standby appliances.

   – **Subnet Mask**: Enter the subnet mask provided by your system administrator.

   – **Gateway**: (Optional) Enter the Gateway provided by your system administrator.

f. **Eth1**: This port is disabled by default. You can enable and configure the Eth1 port for remote Internet connections to the Cisco PAM Server Administration utility.

   – **Enable Interface**: Click the check box to enable or disable the Ethernet interface.

   – **DHCP**: Click the check box to enable or disable DHCP. When DHCP is enabled, the IP following address fields are inactive since the information is supplied by a DHCP server.

   – **IP Address**: Enter the IP address for the Eth0 port. If configured, this address must be different on the active and standby appliances.

   – **Subnet Mask**: Enter the subnet mask provided by your system administrator.

   – **Gateway**: (Optional) Enter the Gateway provided by your system administrator. If a Gateway is provided for Eth0, leave this field blank.

g. Select **Next** to apply the settings and continue.

Tip Either the Eth0, Eth1 or Shared IP address can be used to connect a PC to the Cisco PAM Server Administration utility over the Internet. Ask your system administrator for the IP address used for this purpose in your system.

Step 5 (Optional) Enter the **DNS** Settings for the Cisco PAM appliance. Enter the same settings on the active and standby appliance.

a. **Primary DNS**: (Optional) Enter the domain name server (DNS) for the Cisco PAM appliance.

b. **Secondary DNS**: (Optional) Enter the secondary DNS.

c. **Domain**: (Optional) Enter the domain name for the appliance.

d. Select **Next** to apply the settings and continue.

Step 6 (Optional) Enter the email settings used to send messages from the Cisco PAM appliance. Enter the same settings on the active and standby appliance.

a. **SMTP Server Address**: Enter the SMTP server address used to send outgoing messages. Outgoing messages include event and other alarm information.

b. **SMTP Email Address from**: Enter the email address that will appear in the From field for messages sent by the Cisco PAM appliance. This email address is also the Reply To address.

c. **Test**: Click the Test button to send a test message and verify the SMTP settings. The test message is sent to the administrator email address entered in User settings.

d. Select **Next** to apply the settings and continue.

Step 7 Enter the date and time settings. Enter an initial date and time for the server. These settings are used by the appliance and the Cisco Physical Access Gateways. Enter the same settings on the active and standby appliance.

e. **Date & Time**: Click the calendar icon to open a pop-up window and select the current day. The current date and time are inserted from your computer's date and time settings.

f. **Time Zone**: Select the time zone where the appliance is installed.

g. **NTP enable**: Select the checkbox to enable settings for an optional Network Time Protocol server, used to automatically adjust the date and time settings.

h. **NTP Server Address**: If NTP is enabled, enter the NTP server IP address.

i. Select **Next** to apply the settings and continue.

Step 8 (Optional) Install additional software license using one of the following methods.

- Option 1: Enter the Product Authorization Key to Download the License File, page 4-9.
- Option 2: Obtain the License File from the Cisco Web Site, page 4-10.

Note Enter all licenses except high availability (HA) on the active appliance. Enter only the HA license on the standby appliance. See Licenses in a Redundant Configuration, page 4-15 for more information.

Option 1: Enter the Product Authorization Key to Download the License File

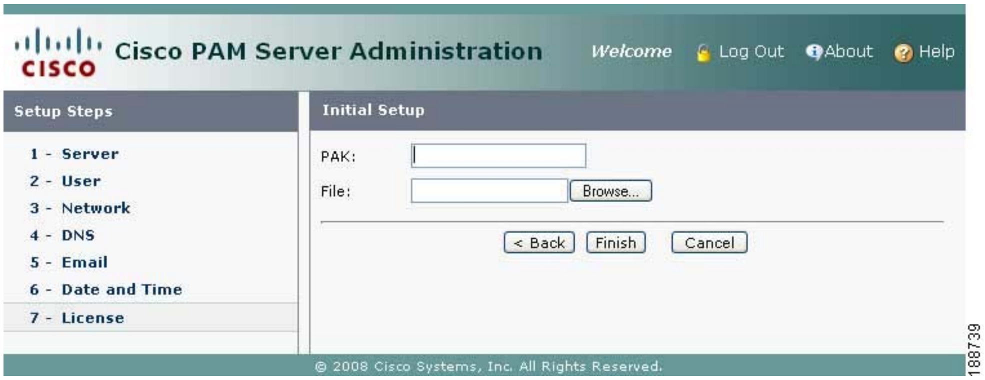
To use this method, your PC must be connected to the Internet.

a. Locate the Product Authorization Key (PAK) included with the Cisco PAM appliance or purchased separately. See Purchasing Additional Feature Licenses, page 4-16.

b. Enter the code in the PAK field, as shown in Figure 4-5.

c. Select **Finish** to download and install the license file on the appliance and activate the features.

Figure 4-5 Initial Setup: License Installation



Note If the license file does not download, verify that your PC has Internet access, or use the following method to download the file from the Cisco Web site.

Option 2: Obtain the License File from the Cisco Web Site

To use this method, obtain the license file from the Cisco Web site using a PC connected to the Internet, and transfer the file to the workstation used for server configuration.

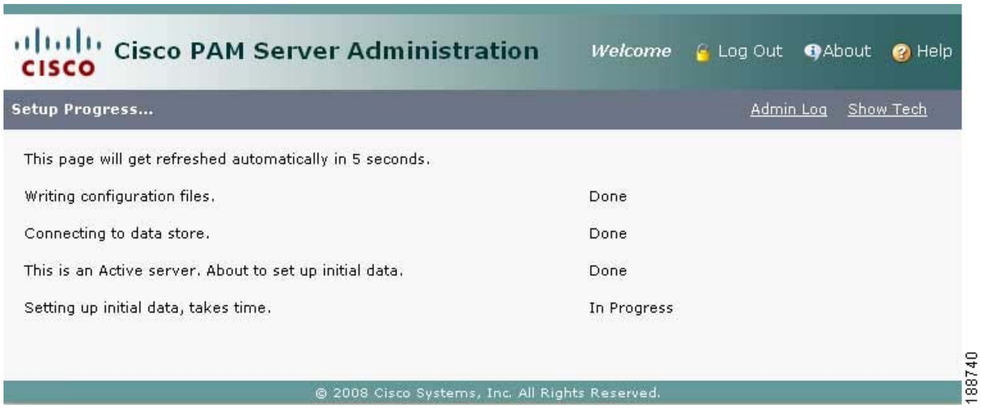
- **a.** Locate the Product Authorization Key included with the Cisco Physical Access Manager appliance or purchased separately. See Purchasing Additional Feature Licenses, page 4-16.
- **b.** In a Web browser, open the Cisco Product License Registration Web page.

  http://www.cisco.com/go/license/
- **c.** Follow the onscreen instructions to complete the form and enter the Product Authorization Key (PAK). When you are done, a license file with the extension `.lic` is sent to your email address.
- **d.** Transfer the file to the drive of the PC used for the configuration.
- **e.** In the License screen (Figure 4-5), click Browse to select the license file located on your local drive. when you select the file, the file name appears in the File field.
- **f.** Select **Finish** to install the license file on the Cisco PAM appliance and activate the features.

Step 9 When you click **Finish**, the initial installation is applied, as shown in Figure 4-6. Click **Done** when all fields read `Done`.

Note If any errors occur, the setup returns to Step 2. If a serious error occurs, contact your Cisco support representative for assistance.

Figure 4-6 Initial Setup: Setup Progress


Cisco PAM Server Administration
Welcome
Log Out
About
Help
Admin Log
Show Tech
© 2008 Cisco Systems, Inc. All Rights Reserved.
188740

Setup Progress...

This page will get refreshed automatically in 5 seconds.

Writing configuration files.	Done
Connecting to data store.	Done
This is an Active server. About to set up initial data.	Done
Setting up initial data, takes time.	In Progress

Step 10 Create a system backup as described in Appendix A, "Backing Up and Restoring Data". You should have at least one backup file to preserve critical system data. You also must have at least one backup to restore the server software using the recovery CD.

Step 11 Disconnect your PC from the Eth0 port and connect the Eth0 port to the IP network.

Performing Additional Configuration, Administration, and Monitoring Tasks

After the initial setup is complete, you can log into the Cisco PAM Server Administration utility to monitor the appliance or modify the configuration. The utility also includes commands to perform tasks such as rebooting the server, backing up data, and installing additional software. You can log in to the administration utility using either a direct connection, or through the Internet using the IP address configured for the Eth0 or Eth1 port.

To use the Cisco PAM Server Administration utility, do the following:

Step 1 Log on to the appliance over the Internet or by using a direct connection:

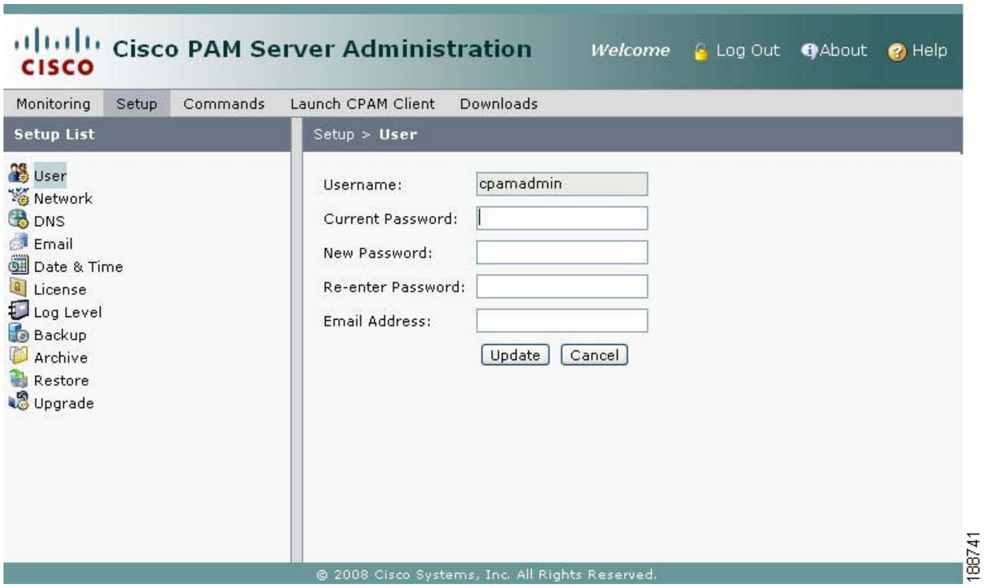
- For a direct connection, see Connecting a PC to the Appliance, page 4-4.
- For an Internet connection, open a web browser and enter the IP address used for the Cisco PAM Server Administration utility. See Logging on to the Cisco PAM Server Administration Utility, page 4-2, or ask your system administrator for assistance.

Note The administration screens also appear immediately following the initial setup.

Step 2 Select a menu from the tabs along the top of the window, as shown in Figure 4-7. Each tab includes additional selections on the left, or additional drop-down menus.

Step 3 Select an option or command as described in Table 4-1 “Menus and Options in the Cisco PAM Server Administration Utility”.

Figure 4-7 Cisco PAM Server Administration Utility: Setup Menus



Username: cpamadmin

Current Password:

New Password:

Re-enter Password:

Email Address:

Table 4-1 described the configuration, administration, and monitoring tasks available in the Cisco PAM Server Administration utility.

Table 4-1 Menus and Options in the Cisco PAM Server Administration Utility

Menu	Description
Monitoring	Displays information about the current and past state of the server, and includes the following submenus: • **Server Status**: Displays real-time information about the current state of the Cisco PAM appliance. Includes the server software version and serial number. • **Server Log**: Displays real-time information regarding server tasks. • **Server Setup Log**: Displays real-time information regarding server setup tasks performed on the appliance. • **Admin Log**: Displays real-time information regarding events related to server administration tasks. • **Admin Audit Log**: Displays a history of tasks performed by the administrator username. • **Server Console Log**: Displays a real-time console log. • **HA Audit**: Displays real-time events related to a redundant server configuration.

Table 4-1 Menus and Options in the Cisco PAM Server Administration Utility (continued)

Setup	Allows you to view and edit the server configuration using the following submenus: • **User**: the username, password and email of the administrator login. • **Network**: the IP address configuration for the appliance and for the Eth0 and Eth1 network ports. See Entering the Initial Server Configuration, page 4-4 for more information. • **DNS**: the DNS settings for the appliance, if DNS is used. • **Email**: the email settings for the appliance, including **SMTP Server Address** and **SMTP Email Address from**. These settings are used to send notifications and other information from the server. – Click **Test** to send a test message and verify the settings. The test message is sent to the administrator email address entered in User settings. – Select **Update** to apply the settings. • **Date & Time**: the server date and time settings. If a network time protocol server is used, click **NTP enable** and enter the **NTP Server Address** settings. • **License**: displays the Cisco licenses installed on the appliance and allows you to install additional licenses. – **Install**: Install additional Cisco Physical Access Control feature licenses. See Obtaining and Installing Optional Feature Licenses, page 4-15. – **Features**: Displays the licensed modules currently installed in the appliance. – **Files**: Lists the license files installed on the appliance. • **Log Level**: Defines the log level for capturing log messages. Select a level for each log subject (such as Security). The log levels are Debug, Info, Warn, Error, and Fatal • **Backup**: creates a compressed backup file of all system and configuration data that can be used to **Restore** a server. To create the backup, enter and re-enter the administrator password and click **Start Backup**. When the operation is complete, the `.zip` backup filename is listed at the top of the screen and the file is stored on the appliance disk. Backup filenames includes the date and the server software version number. To save the file to another location, right-click the filename and select a save option from the browser menu. See Appendix A, "Backing Up and Restoring Data". • **Archive**: removes old events from the system to a password protected `.zip` file containing a SQL script. The SQL script can be run on an offline database to view the purged events. Enter the number of days. Any events older than the number of days entered in this window will be archived. • **Restore**: allows you to restore data from a backup file. To perform a system restore, select **Stop Server** from the Commands menu, enter the administrator password and then click **Browse** to select a backup file. See Appendix A, "Backing Up and Restoring Data". • **Upgrade**: Upgrades the server software. To upgrade the server, select **Stop Server** from the Commands menu, click **Browse** to select an upgrade file, and then click **Upgrade**. Select **Start Server** from the Commands menu when the upgrade is complete. See Appendix B, "Upgrading Software and Firmware".

Table 4-1 Menus and Options in the Cisco PAM Server Administration Utility (continued)

Commands	Provides commands to stop, start and reboot the server. Also includes commands to gather current information from a running server for use in troubleshooting and monitoring. This menu includes the following: • **Start Server**: Enables the Cisco PAM access control server functions and user logins. • **Stop Server**: Disables the Cisco PAM access control server functions. All user logins are denied. The appliance remains in operation and you can still log in to the Cisco PAM Server Administration utility using a direct connection. To restart the access control server, select **Start Server**. • **Reboot**: Performs a hard reboot of the appliance which restarts the OS and the access control server. • **Shut Down**: Shuts down the appliance. All access control functions stop unless a standby appliance is installed and configured. To restart the appliance and access control server, you must physically power down and then power on the appliance. • **Show Tech**: Collects detailed information and logs for use by Cisco technical support. Running this command is processor intensive and can result in decreased system performance. Use the Show Tech command only under the instruction of a Cisco support representative. • **Processes**: Displays the processes running on the system. For use in troubleshooting.
Launch Client	Launches the Cisco PAM desktop client. If the client is not installed or is out of date on your workstation, an installation screen appears. follow the onscreen prompts to install or upgrade the desktop client (if necessary), and launch the application. **Note** If necessary, the required Java application is also installed. This link is the same as the client installation link on the log in page (Figure 4-2) and in the Downloads menu.
Downloads	Provides links to download additional software, including the following: • **Install/Launch Java Runtime Environment for Windows**: Installs only the required version of the JRE (Java Runtime Environment) on a Windows PC. • **Cisco PAM Client Installer Cross Platform (Install Java First)**: Installs Java, and then installs the Cisco PAM desktop client. This link is the same as the client installation link on the log in page (Figure 4-2). • **Install/Launch Cisco VSM Video Player**: Installs the video player required for video integration. See Chapter 15, "Configuring Video Monitoring" for more information. This link is the same as the client installation link on the log in page (Figure 4-2). • **EDI Studio Installer (Install Java First)**: Installs the EDI studio required to configure data integration. See Chapter 14, "Enterprise Data Integration (EDI)" for more information. This link is the same as the client installation link on the log in page (Figure 4-2).

Obtaining and Installing Optional Feature Licenses

The Cisco PAM appliance includes a base package of software licenses to enable access control. To enable additional licensed features, such as the Badge Designer and support for additional hardware modules, complete the instructions in this section. The menus for licensed software features do not appear unless the license is installed on the Cisco PAM appliance

If you are installing a new server, or reconfiguring a server after a system restore from a CD/DVD, see Entering the Initial Server Configuration, page 4-4 to install licenses during the initial setup.

Note Licenses installed on a Cisco PAM appliance cannot be transferred to another appliance. Licenses installed in a redundant (high availability) configuration are automatically transferred from the active appliance to the standby server during a failover.

This section includes the following topics:

- Understanding Module Licenses, page 4-15
- Licenses in a Redundant Configuration, page 4-15
- Purchasing Additional Feature Licenses, page 4-16
- Installing Additional Licenses, page 4-17
  - Option 1: Enter the Product Authorization Key to Download the License File, page 4-17.
  - Option 2: Obtain the License File from the Cisco Web Site, page 4-18.
- Displaying the Cisco PAM Appliance Serial Number, page 4-19
- Displaying a Summary of Installed Licenses, page 4-19

Understanding Module Licenses

Module licenses can be installed to support 64, 128, 256, or 512 hardware modules. Modules include the Cisco Physical Access Control hardware, including the Gateway, Reader, Input and Output modules.

By default, the Cisco PAM appliance supports up to four Cisco hardware modules. To add additional capacity to your system, you must purchase and install additional module licenses. See Part Numbers for the Optional Feature Licenses, page 4-16 for more information.

Module licenses are cumulative: each additional licence is added to the capacity of existing licenses. For example, if you initially installed a 64 module license, you can purchase an additional 128 module license to support a total of 192 Gateways.

Licenses in a Redundant Configuration

If two appliances are installed in a redundant configuration, all installed licenses apply to both the active and standby appliances. If a failover occurs, the standby appliance automatically assumes all active licenses.

Only the high availability (HA) license is installed on the standby appliance. All other licenses are installed on the active server. See Entering the Initial Server Configuration, page 4-4.

Purchasing Additional Feature Licenses

To purchase additional licenses, do the following:

Step 1 Determine the part numbers for the optional licenses you want to purchase. See Table 4-2: Optional Feature Licenses and Part Numbers.

Step 2 Determine the Cisco PAM appliance serial number required to complete the purchase. See Displaying the Cisco PAM Appliance Serial Number, page 4-19 for more information.

Step 3 Purchase the licences by contacting your Cisco sales representative or any Cisco reseller. For more information, visit http://www.cisco.com/en/US/ordering/index.shtml.

Step 4 When the purchase is complete, you are issued a Product Authorization Key (PAK) in paper form, or in an email message.

Step 5 Continue to Installing Additional Licenses, page 4-17 for information on the two options used to download and install the license file using the PAK number.

Part Numbers for the Optional Feature Licenses

Table 4-2 lists the part numbers for the optional feature licenses.

Table 4-2 Optional Feature Licenses and Part Numbers

Part	Optional Feature Licence
CIAC-PAME-M64=	Cisco Physical Access Manager 64-module capacity upgrade license
CIAC-PAME-M128=	Cisco Physical Access Manager 128-module capacity upgrade license
CIAC-PAME-M512=	Cisco Physical Access Manager 512-module capacity upgrade license
CIAC-PAME-M1024=	Cisco Physical Access Manager 1024-module capacity upgrade license
CIAC-PAME-BD=	Cisco Physical Access Manager Badge Designer and Enroller
CIAC-PAME-HA=	Cisco Physical Access Manager High-Availability License
CIAC-PAME-EDI=	Cisco Physical Access Manager Enterprise Data License

Installing Additional Licenses

If your PC is connected to the Internet, you can enter the Product Authorization Key (PAK) to download and install a license file. You can also install a license file stored on a local disk.

Note This section contains instructions to download and install additional license files after the Cisco PAM appliance is set up. If you are installing a new appliance, see Entering the Initial Server Configuration, page 4-4.

This section includes the following information:

- Option 1: Enter the Product Authorization Key to Download the License File, page 4-17
- Option 2: Obtain the License File from the Cisco Web Site, page 4-18

Option 1: Enter the Product Authorization Key to Download the License File

To use this method, your PC must be connected to the Internet.

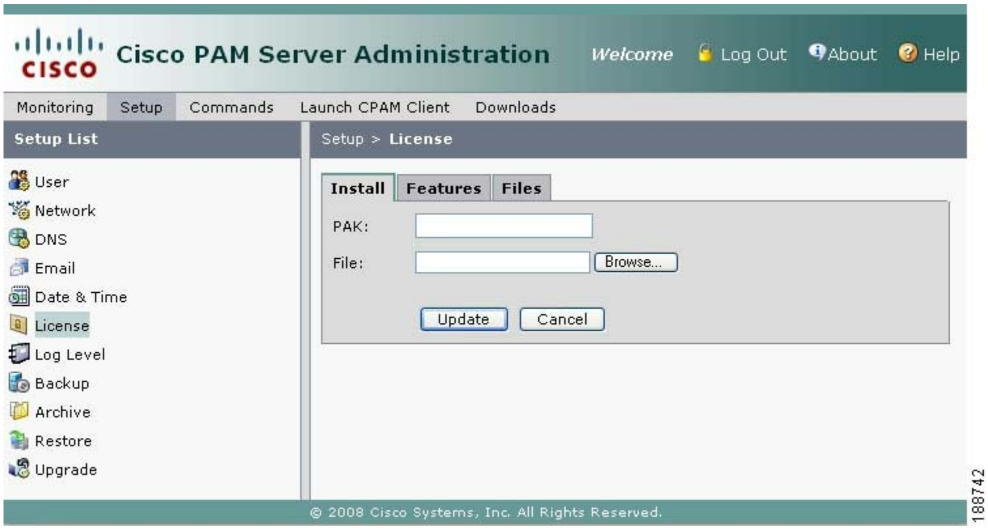
Step 1 Locate the Product Authorization Key (PAK) created with the purchase of the optional feature.

Step 2 Log on to the Cisco PAM appliance as described in Logging on to the Cisco PAM Server Administration Utility, page 4-2.

Step 3 Enter the **PAK** code, as shown in Figure 4-8.

Step 4 Select **Update** to download and install the license file on the appliance and activate the features.

Figure 4-8 Installing Optional Feature Licenses



Note If the license file does not download, verify that your PC has Internet access, or use the method described in Option 2: Obtain the License File from the Cisco Web Site, page 4-18.

Step 5 Select the **Features** tab to verify that the new license was added. See Displaying a Summary of Installed Licenses, page 4-19 for more information.

Step 6 Quit and relaunch the Cisco PAM desktop software to access the new feature menus.

Option 2: Obtain the License File from the Cisco Web Site

To use this method, obtain the license file from the Cisco Web site using a PC connected to the Internet, and transfer the file to the workstation used for server configuration.

Step 1 Locate the Product Authorization Key (PAK) created with the purchase of the optional feature.

Step 2 In a Web browser, open the Cisco Product License Registration Web page.

http://www.cisco.com/go/license/

Step 3 Follow the onscreen instructions to complete the form and enter the Product Authorization Key (PAK). When you are done, a license file with the extension `.lic` is sent to your email address.

Step 4 Transfer the file to the drive of the PC used for the configuration.

Step 5 In the License screen (Figure 4-8 on page 4-17), click **Browse** to select the license file located on your local drive. When selected, the file name appears in the File field.

Step 6 Select **Update** to install the license file on the Cisco PAM appliance and activate the features.

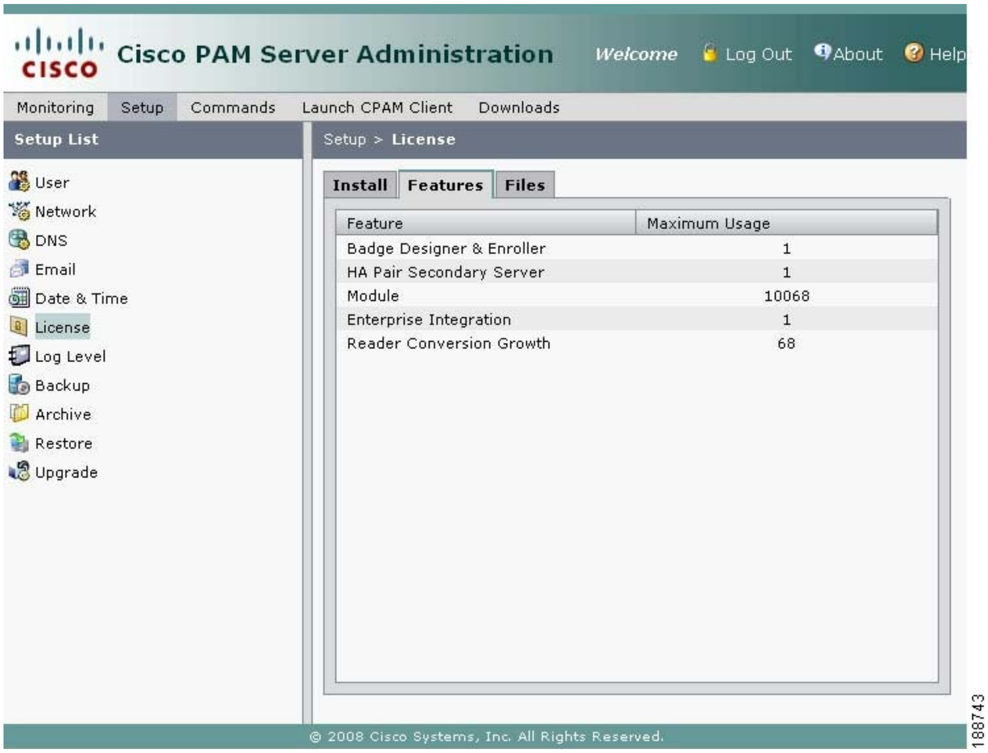
Step 7 Select the **Features** tab to verify that the new license was added. See Displaying a Summary of Installed Licenses, page 4-19 for more information.

Step 8 Quit and relaunch the Cisco PAM desktop software to access the new feature menus.

Displaying a Summary of Installed Licenses

From the Cisco PAM Server Administration utility, select the Features tab in the Setup menu to view a list of installed feature licenses, as shown in Figure 4-9.

Figure 4-9 License Features List



Feature	Maximum Usage
Badge Designer & Enroller	1
HA Pair Secondary Server	1
Module	10068
Enterprise Integration	1
Reader Conversion Growth	68

Displaying the Cisco PAM Appliance Serial Number

To view the appliance serial number, do the following:

Step 1 Log on to the Cisco PAM Server Administration utility:

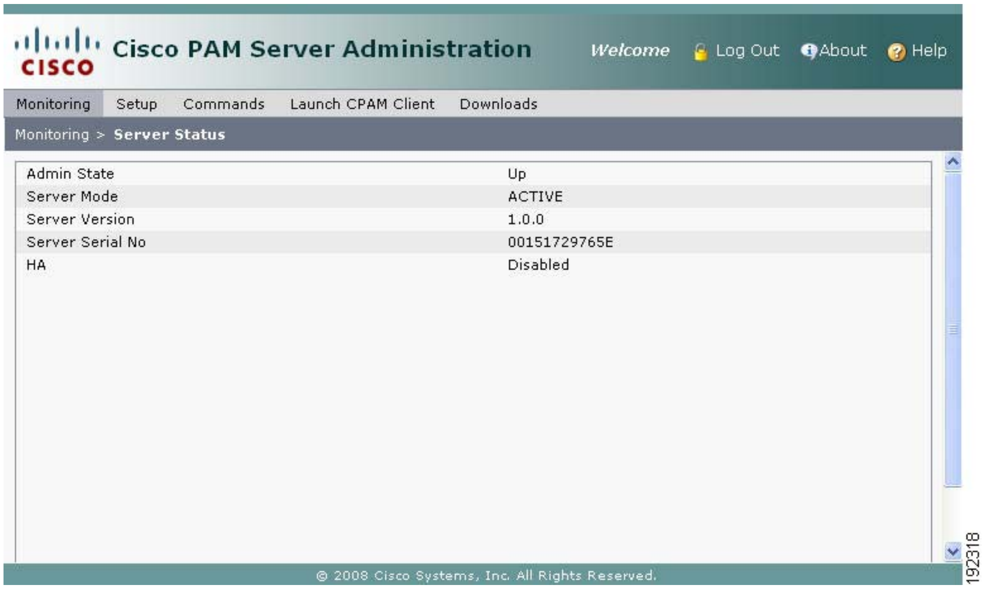
- For a direct connection, see Connecting a PC to the Appliance, page 4-4.
- For an Internet connection, open a web browser and enter the IP address used for the Cisco PAM Server Administration utility. See Logging on to the Cisco PAM Server Administration Utility, page 4-2, or ask your system administrator for assistance.

Note The administration screens also appear immediately following the initial setup.

Step 2 Select the Monitoring tab, and then select Server Status, as shown in Figure 4-10.

Step 3 Refer to the entry for Server Serial No.

Figure 4-10 Cisco PAM Appliance Serial Number


Cisco PAM Server Administration
Welcome
Log Out
About
Help
Monitoring
Setup
Commands
Launch CPAM Client
Downloads
Monitoring > Server Status
© 2008 Cisco Systems, Inc. All Rights Reserved.
192318

Admin State	Up
Server Mode	ACTIVE
Server Version	1.0.0
Server Serial No	00151729765E
HA	Disabled

Performing a Graceful Failover with Redundant Appliances

An automatic failover from the active appliance to the standby appliance occurs if the active appliance goes offline.

To trigger a graceful failover, stop the active appliance. Log on to the Cisco PAM Server Administration utility on the active appliance, and select **Stop Server**, **Restart Server**, **Reboot**, or **Shut Down**. See Performing Additional Configuration, Administration, and Monitoring Tasks, page 4-11 for more information.

Caution A system failover can result in a temporary loss of data. Log and other system messages sent from the Access Gateways and other hardware components may be dropped during the failover process. Cisco recommends performing a manual failover only when system usage is low.

Cisco PAM TCP Port Requirements for Firewall Connections

Table 4-3 lists the TCP ports used by the Cisco PAM appliance. Cisco PAM desktop clients require access to these ports when connectiong to a Cisco PAM appliance that is behind a firewall.

Table 4-3 Cisco PAM Appliance Ports: Firewall Requirements

Port	Description
TCP 80	HTTP for video and redirect to HTTPS
TCP 443	HTTPS
TCP 1236	BVCONTROL
TCP 3306	MYSQL
TCP 8020	Default port for Gateway to Cisco PAM communication

Troubleshooting and Monitoring

See Performing Additional Configuration, Administration, and Monitoring Tasks, page 4-11 for information on the monitoring and troubleshooting features available in the Cisco PAM Server Administration utility. Most of the functions are used to gather information for Cisco technical support. For more information, contact your Cisco support representative.

⚠ **Caution** Using the **Show Tech** command is processor intensive and can result in poor system performance while the information is gathered from your system, Use the **Show Tech** command under the direction of a Cisco technical support representative only.

Next Steps

When the initial setup is complete, the Cisco PAM appliance is ready to configure the access control features of your system, including doors, users, badges, and other features. See Chapter 5, "Getting Started With the Cisco PAM Desktop Software" for instructions to log in and get started.

For information on installing and configuring the Access Gateway and other physical modules, see the *Cisco Physical Access Gateway User Guide*.