Installing and Configuring the Cisco Physical Access Gateway

Contents

This chapter includes the following information:

• Overview, page 2-2
• Package Contents, page 2-3
• Physical Overview and Port Description, page 2-3
• Installing the Cisco Physical Access Gateway, page 2-7
• Configuring and Managing the Gateway Using a Direct Connection, page 2-15
  – Understanding Network Time Protocol (NTP) Settings, page 2-15
  – Connecting a PC to the Gateway, page 2-16
  – Entering the Gateway Network Settings, page 2-17
  – Changing the User Password, page 2-19
  – Upgrading the Gateway Firmware Using a Direct Connection, page 2-20
  – Displaying Serial Numbers and Other Information, page 2-23
• Configuring the Gateway Using the Cisco Physical Access Manager, page 2-24
• Resetting the Cisco Physical Access Gateway, page 2-25
Overview

The Cisco Physical Access Gateway (Figure 2-1) is installed near each door to provide access control and connections for card readers, door locks and other input and output devices. The Gateway is connected to the Cisco Physical Access Manager using an Ethernet connection to the IP network. Power is supplied through a Power over Ethernet (PoE) connection, or using a DC power source. Each Gateway includes connections for up to two Wiegand door readers, three input devices, and three output devices. Optional expansion modules are available to add additional doors and devices to the Gateway.

Figure 2-1  Cisco Physical Access Gateway
Package Contents

Each Cisco Physical Access Gateway includes the following:

- Six End-Of-Line (EOL) 1K termination resistors (used for supervised input interfaces)
- Two mounting brackets, with 4 screws for each bracket
- Regulatory compliance and safety information
- Quick Start guide
- Connector plugs, including the following:

<table>
<thead>
<tr>
<th>Type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Pin</td>
<td>1</td>
</tr>
<tr>
<td>3 Pin</td>
<td>4</td>
</tr>
<tr>
<td>2 Pin</td>
<td>6</td>
</tr>
</tbody>
</table>

Physical Overview and Port Description

Figure 2-2 and Figure 2-3 show the location of each port, including connections for power, Ethernet, door readers and other input and output devices.

Figure 2-2  Cisco Physical Access Gateway Ports and Connectors: Side View
**Physical Overview and Port Description**

**Figure 2-3  
Cisco Physical Access Gateway Ports and Connectors: Top View**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power—Two-pin connector for Voltage In (VIN) and Ground (GND) to connect a 12 to 24 VDC external power source.</td>
</tr>
<tr>
<td>2</td>
<td>CAN—A three-wire CAN bus is used to connect additional modules, including the Cisco Reader Module, Cisco Input Module, and Cisco Output Module. <strong>Note</strong> Modules are connected using the CAN1 interface. The CAN2 interface is not supported in this release.</td>
</tr>
<tr>
<td>3</td>
<td>SVR (Server)—When the LED is steady green, the Gateway is connected to a Cisco PAM appliance.</td>
</tr>
</tbody>
</table>
| 4 | Fast Ethernet interfaces—There are two 10/100 BASE-TX RJ-45 connectors:  
  * **ETH 0**: connects the Gateway to the network. ETH 0 also supports Power over Ethernet (PoE) for the device (optional).  
  * **ETH 1**: connects the device to a PC to access the device configuration web page. |
| 5 | Serial interface—The RS-485 interface is not supported in this release. |
| 6 | Wiegand interface—This interface can be configured as the following:  
  * One 10-pin Wiegand/clock and data reader interface to connect a single door reader.  
  * Two 5-pin Wiegand/clock and data interfaces to connect two door readers (for installations where a 5-pin interface is sufficient). **Note** Disconnect power from the Gateway or Reader module before connecting reader devices to the modules. Connecting a reader device when the modules are powered can cause the Gateway or Reader module to malfunction. |
Table 2-1 describes the Gateway module status LEDs:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVR</td>
<td>Steady Green The Gateway is connected to a Cisco PAM appliance.</td>
</tr>
</tbody>
</table>

LED Status
### Table 2-1 Gateway LEDs (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Port LEDs</strong></td>
<td></td>
</tr>
<tr>
<td>OFF</td>
<td>Input is not configured</td>
</tr>
<tr>
<td>GREEN</td>
<td>Input is configured and in normal state</td>
</tr>
<tr>
<td>BLINKING GREEN</td>
<td>Input is configured, and is receiving and alarm or other data.</td>
</tr>
<tr>
<td>BLINKING RED</td>
<td>Input is configured, short</td>
</tr>
<tr>
<td>RED</td>
<td>Input is configured, open</td>
</tr>
<tr>
<td><strong>Output Port LEDs</strong></td>
<td></td>
</tr>
<tr>
<td>Off</td>
<td>Output not configured</td>
</tr>
<tr>
<td>Solid Green</td>
<td>Output configured and in default state</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Output configured and active</td>
</tr>
</tbody>
</table>

**Note**

Led Status does not work on 5 wire reader.
Installing the Cisco Physical Access Gateway

- Before You Begin, page 2-7
- Procedure, page 2-7

Before You Begin
Before you install a Cisco Physical Access Gateway, verify the following:

- Verify that the module has access to a power source. See the “Power Options and Requirements” section on page 1-12 for more information.
- Verify that you have the necessary mounting brackets or other hardware. See the “Mounting a Gateway or Optional Module” section on page 1-14.

Procedure
To install the Cisco Physical Access Gateway, perform the following procedure:

**Step 1** Mount the Gateway to a wall. See the “Mounting a Gateway or Optional Module” section on page 1-14 for more information.

**Step 2** Connect the Gateway to a power source.

- If using a DC power source, insert a two-pin connector plug into the DC power port (Figure 2-4), and connect the Voltage In (VIN) and ground (GND) wires.
- If using PoE, connect an Ethernet cable from the IP network to the ETH0 port (Figure 2-4).

See the “Power Options and Requirements” section on page 1-12 for more information.
Installing the Cisco Physical Access Gateway

Figure 2-4  Power Connections for the Cisco Physical Access Gateway

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DC power GND (ground)—Connects the DC ground wire to the Gateway.</td>
</tr>
<tr>
<td>2</td>
<td>DC power Voltage In (VIN)—Connects the DC Voltage In (VIN) wire to the Gateway.</td>
</tr>
<tr>
<td>3</td>
<td>ETH0 for PoE—Connects the Ethernet cable from the Access Layer switch to the Gateway. To use this power option, the switch must support PoE.</td>
</tr>
</tbody>
</table>

Step 3  Connect one or two door reader devices to the Wiegand interface using one of the following configurations:

- Connect a single door reader using all 10 Wiegand interface pins.
- Connect one or two door readers using 5-pin Wiegand interface connections (for installations where a 5-pin interface is sufficient).
Figure 2-5 shows the location of the Wiegand interface connections. The table describes the connections for 10-pin and 5-pin reader interface connections. The wire connectors from the reader device are shown in parentheses. If attaching a second reader, use the alternative connections shown in the column on the far right.

**Figure 2-5  Wiegand Interface on the Gateway and Reader Modules**

<table>
<thead>
<tr>
<th>Chassis Label</th>
<th>Description</th>
<th>One Reader 10 Wire Connection</th>
<th>First Reader in a 5 Wire Connection</th>
<th>Second Reader in a 5 Wire Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PWR</td>
<td>+12v</td>
<td>PWR (red)</td>
<td>PWR (red)</td>
<td>PWR (red)</td>
</tr>
<tr>
<td>2 GND</td>
<td>Ground</td>
<td>GND (black)</td>
<td>GND (black)</td>
<td>GND (black)</td>
</tr>
<tr>
<td>3 D0</td>
<td>Data 0</td>
<td>D0 (green)</td>
<td>D0 (green)</td>
<td>---------</td>
</tr>
<tr>
<td>4 D1/CLCK</td>
<td>Data 1</td>
<td>D1/CLCK (white)</td>
<td>D1/CLCK (white)</td>
<td>---------</td>
</tr>
<tr>
<td>5 DRTN</td>
<td>Shield</td>
<td>DRTN (shield)</td>
<td>DRTN (shield)</td>
<td>DRTN (shield)</td>
</tr>
<tr>
<td>6 GRN</td>
<td>Output 2</td>
<td>GRN (orange)</td>
<td>GRN (orange)</td>
<td>---------</td>
</tr>
<tr>
<td>7 RED</td>
<td>Output</td>
<td>RED (brown)</td>
<td>---------</td>
<td>GRN (orange)</td>
</tr>
<tr>
<td>8 BPR</td>
<td>Output (Beeper)</td>
<td>BPR (yellow)</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
Step 4 Connect input devices to the Gateway:

a. Insert two-pin connector plugs into the input ports (see Figure 2-7).

b. (Optional, for supervised input connections only). Install two End-Of-Line (EOL) 1K termination resistors in each supervised input interface (one terminator in each connector). Figure 2-6 shows the terminator installation for a Normally Closed (NC) and Normally Open (NO) input connection.

c. Connect the wires from the input devices (see Figure 2-7).

Note Each of the input connections can be configured as supervised or unsupervised. The tamper and power fail inputs can be configured as additional unsupervised ports. A supervised input supports four states: normal, alarm, open and short. An unsupervised input indicates only normal or alarm.
Step 5  Connect output devices to the Gateway (Figure 2-8). Each of the three Form C (5A @ 30V) relay output connections can be configured as either Normally Closed (NC) or Normally Open (NO).

a. Insert three-pin connector plugs into the output ports.

b. Connect the wires from the output devices.

- Common (C) is always used, and either NC or NO is used to complete the connection.
- If the relay is normally open, use the C & NO connections. The circuit is closed when triggered.
- If the relay is normally closed, use the C & NC connections. The circuit is opened when triggered.
Step 6  Connect optional expansion modules to the Gateway, if necessary:

a. Insert a three-pin connector plug into the CAN1 port, as shown in Figure 2-9.

b. Connect the CAN wires to the CAN bus, as shown in Figure 2-10.

c. On the last device in the CAN bus, set the CAN terminator switch to ON. The CAN terminator switch is included on the Reader, Input and Output modules only (the Gateway is always the first device in the CAN bus). Set the terminator switch to OFF for all other modules in the CAN bus.

Note  Modules are connected using the CAN1 interface. The CAN2 interface is not supported in this release.
Figure 2-9  CAN1 Connections: Cisco Physical Access Gateway and Reader Module

1  CAN+
   Connects to the positive terminal of the CAN bus.

2  CAN-
   Connects to the negative terminal of the CAN bus.

3  Shield
   Connects to GND and/or Shield.

Note
On the last device in the CAN bus, set the CAN terminator switch to ON. The CAN terminator switch in included on the Reader, Input and Output modules only (the Gateway is always the first device in the CAN bus).
Step 7  Connect the Gateway to the IP network by connecting an Ethernet cable to the ETH0 port, as shown in Figure 2-11.

Figure 2-11 ETH0 Ethernet Connection for the Cisco Physical Access Gateway

<table>
<thead>
<tr>
<th>1</th>
<th>ETH0—Ethernet port for connecting the Gateway to the IP network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>The ETH0 connection can also be used for Power over Ethernet.</td>
</tr>
<tr>
<td>Note</td>
<td>The ETH1 port is used to connect a PC to the Gateway for configuration and monitoring. See the “Configuring and Managing the Gateway Using a Direct Connection” section on page 2-15 for more information.</td>
</tr>
</tbody>
</table>

Step 8  Continue to the “Configuring the Gateway Using the Cisco Physical Access Manager” section on page 2-24.
Configuring and Managing the Gateway Using a Direct Connection

To enable the Gateway communication with the Cisco PAM appliance, connect a PC to the ETH1 port and use a web browser to enter basic network settings, as described in this section. You can also use the web administration tool to perform basic administration and monitoring tasks, such as upgrading the module firmware or displaying the module serial number.

This section includes the following information:
- Understanding Network Time Protocol (NTP) Settings
- Connecting a PC to the Gateway
- Entering the Gateway Network Settings
- Changing the User Password
- Upgrading the Gateway Firmware Using a Direct Connection
- Displaying Serial Numbers and Other Information

You can also use the Cisco PAM desktop software to enter network settings and upgrade firmware images. See the “Configuring the Gateway Using the Cisco Physical Access Manager” section on page 2-24.

Understanding Network Time Protocol (NTP) Settings

Cisco Systems strongly recommends using a network time protocol (NTP) server to synchronize the date and time clock on each Gateway module, and on the Cisco PAM appliance. This ensures that events and messages between the server and the Gateway modules are in sync. If the time and date are not synchronized, inconsistent system behavior can occur.

We strongly recommend using the same NTP server setting for the Cisco PAM appliance, and for all Gateway modules.

- Gateways can receive the NTP server setting from a DHCP server, or by using the Cisco PAM desktop software.
  - To enter the Gateway DHCP settings, see the “Entering the Gateway Network Settings” section on page 2-17.
  - If DHCP is used to define the Gateway NTP server, any NTP settings defined using the Cisco PAM desktop software will not apply (the DHCP configuration takes precedence).
  - To enter the NTP setting for a single Gateway using Cisco PAM desktop software, choose Hardware from the Doors menu, right-click a Gateway module, and choose Set Gateway Address.
  - Beginning with Cisco PAM Release 1.3.0, you can also change the NTP server setting for multiple Gateways (Right-click the Access GW Driver and choose the Set NTP Server command). See the Cisco Physical Access Manager User Guide for instructions.
- To enter the NTP setting on the Cisco PAM server, use the Cisco PAM web administration tool. See the Cisco Physical Access Manager User Guide for instructions.
Chapter 2 Installing and Configuring the Cisco Physical Access Gateway

Connecting a PC to the Gateway

To enter the initial Gateway settings or perform other administration tasks, connect a PC to the Gateway ETH1 port and use a web browser to access the administration pages.

Before You Begin
To configure a Cisco Physical Access Gateway, you need the following:

- A PC and web browser.
  The Cisco Physical Access Gateway supports Internet Explorer 6.0 and higher.
- A Ethernet cable to connect your PC to the Gateway.
  Cross-over and straight-through cables are supported.
- Your PC must be configured to connect to the 192.168.1.0 network using Ethernet. Use any static host address on the network other than 192.168.1.42.
- Power connected to the Cisco Physical Access Gateway.
  See the “Installing the Cisco Physical Access Gateway” section on page 2-7 for more information.

In addition, gather the following information:

- The IP Address of the Cisco PAM appliance.
- You can use a DHCP server to assign an IP address for the Gateway.
  If a DHCP server is not used, gather the Cisco Physical Access Gateway IP address, IP gateway, subnet mask.
- The domain name server (DNS) for the Gateway if DNS names (not IP addresses) are used for the NTP or Cisco PAM addresses.

Procedure
Complete the following steps to log on to the administration tool.

Step 1
Connect an Ethernet cable from a PC to the ETH1 interface on the Gateway module.

- See the “Physical Overview and Port Description” section on page 2-3 for the port location.
- Be sure to connect your PC to the ETH1 port. The ETH0 port is used for network communication.
- Your PC must be configured to connect to the 192.168.1.0 network using Ethernet. Use any static host address on the network other than 192.168.1.42.

Step 2
Open a web browser on your PC and enter https://192.168.1.42 to access the web-based administration pages.

Step 3
Enter the default username and password (Figure 2-12).

  default username: gwadmin
  default password: gwadmin
Chapter 2      Installing and Configuring the Cisco Physical Access Gateway

Configuring and Managing the Gateway Using a Direct Connection

Figure 2-12      Login Screen for the Cisco Physical Access Gateway

The web administration pages appear, and are described in the following sections.

Entering the Gateway Network Settings

Enter the network settings to enable IP communication between the Gateway and the Cisco PAM appliance. Network settings include the following:

- **ETH0 Configuration**: the ETH0 port provides IP network connectivity with the Cisco PAM appliance.
- **DNS Configuration**: enter a DNS configuration if names (not IP addresses) are used for the NTP or CPAM addresses.
- **Cisco PAM Configuration**: defines the IP address and port of the Cisco PAM appliance that is used to manage the Gateway.

Tip

Gateway modules can be added to the IP network before or after the full module configuration is entered in Cisco PAM. For more information, see the Cisco Physical Access Manager User Guide.

Procedure

Complete the following steps for each Gateway in the system.

Step 1

Enter the **ETH0 Configuration** settings, as shown in Figure 2-13. The ETH0 port is used for network communications with the Cisco PAM appliance.

a. If a Dynamic Host Configuration Protocol (DHCP) server is configured on your IP network, check the **DHCP** box for ETH0 to automatically configure the required IP network settings, including IP address, Subnet Mask, and Gateway. The **DHCP** check box is checked by default.

b. (Optional) If a DHCP server is not used to assign IP address settings, enter the following information in the **ETH0** fields:
   - **IP address**: Enter the IP address of the Cisco Physical Access Gateway.
   - **Subnet Mask**: Enter the subnet mask.
   - **Gateway**: Enter the IP gateway address.
Configuring and Managing the Gateway Using a Direct Connection

Figure 2-13  Network Settings for the Cisco Physical Access Gateway

Step 2  (Optional) Enter the DNS Server address if names (not IP addresses) are used for the CPAM address.

Step 3  Enter the Cisco PAM Configuration:

a. Enter the Cisco PAM IP Address (IP address or name) to enable Gateway communication with the appliance.

b. Enter the Port number for the Cisco PAM appliance. The port number must be greater than 1024 and less 65535. The default is 8020.

Tip  DHCP can also be configured to supply the Gateway with the IP address of the Cisco PAM appliance by configuring option 150 in the DHCP response. The Cisco PAM appliance TCP port number can be provided by DHCP option 151 of the DHCP response.

c. Enable SSL: The secure socket layer (SSL) is enabled for secure communication between the Gateway and Cisco PAM appliance by default. If necessary SSL can be disabled by unchecking the Enable SSL check box.

Note  SSL is enabled by default on all Gateways and Cisco PAM appliances. If SSL is disabled for a Gateway but enabled for Cisco PAM, the Gateway will not be able to connect to the appliance. If the SSL settings are changed, reset all Gateways and the Cisco PAM appliance. We recommend enabling SSL to ensure secure communications.

Step 4  Click Save to save the settings. Wait until the Gateway resets and the web browser displays the screen Network Settings Applied. Or click:

- Reset Application: The Reset Application restarts the Gateway to clear any software issues. The Gateway reconnects with the server (CPAM) after reset.

- Reboot: The Reboot command reloads the device firmware and all configuration/settings(re-initialized). This does not impact stored data. Again the Gateway reconnects with the server after reload.
- **Reset Factory Defaults**: This command deletes all information on the device (including log and event data), resets the password and all other configurations to the factory default. Any custom configurations previously entered on the device are also removed.

- **Delete Events**: delete all events stored on the Gateway.

- **Delete Configuration**: delete the module configuration. The configuration is automatically downloaded when the gateway establishes communication with the Cisco PAM appliance.

- **Delete Credentials**: delete the credential data stored on the Gateway. The credential is automatically downloaded when the gateway establishes communication with Cisco PAM appliance.

---

**Note**

- Changes do not take effect until saved.
- Delete Events, Delete Configuration, Delete Credentials includes an application reset of the gateway.

---

**Step 5** Repeat Step 1 through Step 4 for each Gateway in the system.

**Step 6** Perform additional configuration, verification, and monitoring tasks as described in the Cisco Physical Access Manager User Guide.

---

**Changing the User Password**

**Tip** You can also change the password for one or more Gateways using the Cisco PAM desktop software. See the “Changing Gateway Passwords” section in the Cisco Physical Access Manager User Guide for more information.

The Gateway password can be added/reset from CPAM also.
**Procedure**

To change the password used to access the Gateway, perform the following procedure:

---

**Step 1**

Click the User Management tab, as shown in **Figure 2-14**.

**Figure 2-14**  **User Management for the Cisco Physical Access Gateway**

---

**Step 2**

Enter the Current Password.

**Step 3**

Enter the New Password.

**Step 4**

Re-enter the new password to verify the setting.

**Step 5**

Click **Update** to save the changes.

---

**Note**

The username cannot be changed.

**Tip**

To reset the device to the default password, see the “Hard Reset (Restore Factory Defaults)” section on page 2-25.

---

**Upgrading the Gateway Firmware Using a Direct Connection**

---

**Tip**

You can also upgrade the firmware for a single Gateway, or all Gateways, over the network using the Cisco PAM desktop software. For instructions, see the **Cisco Physical Access Manager User Guide**.
Procedure
To upgrade the Gateway firmware from a PC directly connected to the module, perform the following procedure:

Step 1  Log on to the Gateway administration tool, as described in the “Connecting a PC to the Gateway” section on page 2-16.

Step 2  Click the Image Management tab, as shown in Figure 2-15.

Figure 2-15  Image Management for the Cisco Physical Access Gateway

Step 3  Determine the active and running firmware images:

The Image Management window displays all firmware images loaded on the Gateway. The running image is the firmware currently operating the Gateway module. The active image is the image that will become the running image when the Gateway module is reset. The table displays the images currently loaded on the module:

- **Current Images**: a list of the firmware images currently loaded on the Gateway module.
- **Running**: the green check in the Running column indicates the image operating the Gateway.
- **Active**: the green check in the Active column indicates the image set as the active image. This is the image that will become the Running image when the Gateway is reset.

Step 4  Upload a new firmware image from a file located on a local disk or on a remote TFTP server:

You can also choose an existing image: highlight the image name, click the Set Active button, and then reset the Gateway. The new active image becomes the running image only after the Gateway is reset (see the “Soft Reset (Powercycle)” section on page 2-25).
**Option 1: Local Disk**

To upload a firmware file from a local on the connected PC:

a. Select the **Local** radio button, as shown in Figure 2-15.

b. Click **Browse** and choose a file from located on a local or network disk. The selected file appears in the Image Name field. You can also manually enter the directory path and filename.

**Option 2: Remote TFTP Server**

To upload a firmware file from a remote TFTP server:

a. Select the **Remote** radio button.

b. Enter the TFTP Server IP address.

c. Enter the directory Path on the TFTP server for the firmware image. Be sure the path and filename are valid. The administration tool does not verify remote server paths.

| Tip | The directory path and filename for the remote image displays in the second Image Name field. You can also enter the path and filename manually. |

d. Choose the options that will occur after the image is loaded to the Gateway:

| Note | When upgrading Gateway firmware images from a release prior to release 1.1.0, choose all available options. |

- **Active image**: (checked by default) make the firmware file new active image.
- **Reset gateway**: (checked by default) perform a soft reset to powercycle the module. See the “Soft Reset (Powercycle)” section on page 2-25 for more information. Changes to the active image are applied only after the Gateway is reset.
- **Delete credentials**: delete the credential data stored on the Gateway. The credential is automatically downloaded when the Gateway establishes communication with Cisco PAM appliance.
- **Delete configuration**: delete the module configuration. The configuration is automatically downloaded when the Gateway establishes communication with the Cisco PAM appliance.
- **Delete events**: delete all events stored on the Gateway.

**Step 5**

Click **Upgrade** to copy the firmware image to the Gateway module and perform the selected options (if any).

When all options are selected, wait approximately 10-15 minutes for the firmware upgrade to complete.

| Note | The Gateway must be reset to enable the new active image. See the “Soft Reset (Powercycle)” section on page 2-25. |
Displaying Serial Numbers and Other Information

Use the Show Inventory window to display the module serial number and other information, such as the module serial number.

**Step 1** Log on to the Gateway administration tool, as described in the “Connecting a PC to the Gateway” section on page 2-16.

**Step 2** Click the Show Inventory tab, as shown in Figure 2-16.

**Figure 2-16** Show Inventory Window for the Cisco Physical Access Gateway
The serial number is also displayed on the back of the module. To view the serial number in Cisco PAM, open the **Hardware** module device view, right-click on the **Gateway Controller**, and choose **Edit** to view the module properties.

**Configuring the Gateway Using the Cisco Physical Access Manager**

After the initial Gateway configuration is complete, use the The Cisco Physical Access Manager (Cisco PAM) desktop software for advanced configuration of Gateways and other components. For example, you can use Cisco PAM to configure doors, door devices and access policies enabled by the Gateway modules.

In addition, you can use Cisco PAM to do the following:

- Display the network and firmware settings for each Gateway.
- Change the Gateway module network settings.
- Change the NTP setting for multiple Gateway modules.
- Upgrade Gateway firmware images.

See the [Cisco Physical Access Manager User Guide](#) for more information.

---

**Tip**

You can configure the Gateway modules in Cisco PAM before or after they are added to the IP network.
Resetting the Cisco Physical Access Gateway

Reset the Gateway to powercycle the module, restore the factory settings, or delete the stored logs and other data. The effect of the restart depends on the type of restart your perform, as described in the following sections. You can reset the module using the physical button on the side of the module, or in software using either the web administration tool or the Hardware device view in Cisco PAM.

- **Soft Reset (Powercycle), page 2-25**
- **Hard Reset (Restore Factory Defaults), page 2-25**

Soft Reset (Powercycle)

Use the soft reset to powercycle the Cisco Physical Access Gateway. A soft reset reloads the device firmware to clear any software issues, but does not impact stored data. The password, logs and other information are retained.

Use one of the following methods to perform a soft reset:

- **Hardware reset button**: Press and release the reset button once. See Figure 2-2 on page 2-3 for the location of the Reset button.
- **Gateway web administration tool**: Follow the instructions in the “Configuring and Managing the Gateway Using a Direct Connection” section on page 2-15 to connect a PC to the Gateway, and click the Reset button at the bottom of the screen.
- **Cisco PAM desktop software**: Open the Hardware module in the Doors menu and right-click on a Gateway Controller (blue icon). Choose Reset from the menu.

Hard Reset (Restore Factory Defaults)

A hard reset deletes all information on the device (including log and event data) and resets the password and all other configurations to the factory default. Any custom configurations previously entered on the device are removed.

Note the following:

- Allow five to 10 minutes for the hard reset erase operation to complete.
- Do not disconnect power from the module until the hard reset erase process is complete. Loss of power during a hard reset can result in equipment malfunction.
- The SVR LED flashes throughout the erase operation.
- The module reboots with the existing firmware image after the hard reset is complete.

Use one of the following methods to perform a hard reset:

- **Hardware reset button**: Press Reset button three times in succession. See Figure 2-2 on page 2-3 for the location of the Reset button.
- **Gateway web administration tool**: Follow the instructions in the “Configuring and Managing the Gateway Using a Direct Connection” section on page 2-15 to connect a PC to the Gateway, and click the Restore Factory Defaults button at the bottom of the screen.