Understanding Door Configuration

This chapter describes the concepts used to configure doors and templates. A door configuration is a collection of devices, such as locks and readers, connected to a Cisco Physical Access Gateway and configured in Cisco PAM. To configure a door, add a Gateway to Cisco PAM and then assign one or more door configurations to the Gateway using the pre-defined door templates. Door configuration templates include common sets of devices and configurations to simplify access control configuration. Gateways and the associated doors can be configured either before or after the Gateway is added to the network.

Tip

See Installation and Configuration Summary, page 1-3 for a quick summary of tasks.

Door configurations can only include devices not assigned to another door. The configuration wizard only displays unassigned devices. See Chapter 6, “Configuring Doors” for more information.

Contents

- Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2
- Viewing Device and Door Configuration, page 5-3
- Viewing Device and Door Status, page 5-9
- Understanding Door Configurations and Templates, page 5-20
- Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 5-25
- Locating Serial Numbers, page 5-36
- Related Documentation, page 5-37
**Provisioned (Pre-Populated) vs. Discovered Gateway Configurations**

You can configure a Gateway in Cisco PAM before or after the module is added to the network.

- **Provisioned (Pre-Populated) Configuration**, page 5-2
- **Discovered Configuration**, page 5-2

---

**Note**

See also **Configuration Management in Provisioned vs. Discovered Configurations**, page 6-18.

---

**Provisioned (Pre-Populated) Configuration**

A **Provisioned** configuration occurs when a Gateway configuration is entered in Cisco PAM before the module is brought online. If the Gateway serial number matches the existing Cisco PAM configuration when the module is added to the network, Cisco PAM automatically downloads the existing configuration to the module.

- Subsequent changes to the configuration must be manually applied, as described in **Applying Configuration Changes**, page 6-17.
- If the Gateway connects to Cisco PAM and does not have a configuration (such as after a hard reset), the latest configuration applied to that Gateway is downloaded.

**Discovered Configuration**

A **Discovered** configuration occurs when a Gateway is added to the network and no Cisco PAM configuration exists. Cisco PAM automatically creates a new entry based on the module serial number and the serial numbers of any attached expansion modules.

The Gateway is assigned a name based on “gw_” and the serial number. For example, if the Gateway serial number is FHH112900XX, the name of the discovered Gateway configuration in Cisco PAM will be gw_FHH112900XX.

After the Gateway is added, complete the module and door configuration as described in **Chapter 6, “Configuring Doors”**.

---

**Note**

The serial number for each Gateway and expansion module is unique and cannot be changed. In a Discovered configuration, the serial numbers are automatically sent from the module to the Cisco PAM appliance over the IP network. If the serial number for the Gateway or an attached expansion module already exists in the Cisco PAM configuration, the Gateway is not added.
Viewing Device and Door Configuration

A door configuration is a collection of devices, such as locks and readers, connected to a Cisco Physical Access Gateway and configured in Cisco PAM. To configure a door, add a Gateway to Cisco PAM and then assign one or more door configurations to the Gateway using pre-defined door templates. Door configuration templates include common sets of devices and configurations to simplify access control configuration.

Once the Gateways and door configurations are added to Cisco PAM, you can view the configurations in a device view that lists the Gateways, expansion modules, and interfaces, or in a Locations view, that displays the door configurations in a hierarchical location map.

This section includes the following information.

- Viewing Doors and Devices in the Hardware View, page 5-3
- Viewing Doors and Devices by Location, page 5-5
  - Creating the Location Map, page 5-6
  - Filtering the Devices Displayed in the Locations View, page 5-7
  - Changing the Location of a Device or Door, page 5-8

Viewing Doors and Devices in the Hardware View

The Device view in the Hardware module displays a list of configured Gateways, expansion modules, and other devices in a hierarchical tree, as shown in Figure 5-1.

To open the device view, select Hardware from the Doors menu. In the Hardware window, select Device from the View menu. Gateways are listed by name and represented by a blue icon, as shown in Figure 5-1. Click the box next to the icon to expand the hierarchical tree and view the expansion modules and other devices associated with the Gateway.

![Figure 5-1 Expanded Hardware Tree: Gateways and Related Devices](image)

**Note**

Some devices, such as tamper inputs, fire sensors, and cameras, are not part of door configurations.
Tip

The names of all hardware tree elements are editable, including Drivers, Gateways, expansion modules, and door devices.

Table 5-1 describes the icons and drivers shown in Figure 5-1:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Site</td>
<td>Read-only. A site is a single instance of a Cisco PAM database. It generally, but does not necessarily, correspond with a single geographical location, such as a building complex, building, or part of a building. Most installations of Cisco PAM only have a single database, and hence a single site. Multiple sites are used in larger configurations, such as a company with offices in distant locations that have a Cisco PAM database at each office.</td>
</tr>
<tr>
<td>2 Driver Manager</td>
<td>Read-only. The Driver Manager enables Cisco PAM hardware and software drivers, such as the gateway Driver or the EDI Driver. The Driver Manager cannot be deleted.</td>
</tr>
</tbody>
</table>
| 3 Access GW Driver | The Access GW Driver allows you to add Cisco Physical Access Gateway hardware modules to the system configuration, and supports the additional expansion modules (Reader, Input and Output) connected to a Gateway. The Access GW Driver also manages the events and alarms generated by devices, modules, and Gateways. The Access GW Driver is enabled by default.  
Note The Access Gateway Driver is an example of a Device Driver. Device Drivers enable software and hardware functionality. Additional Device Drivers include the Logical Driver, Automation Driver, EDI Driver, and Cisco VSM Driver. Each of these drivers enables the functionality for that feature, and provides basic configuration settings. There can only be one instance of each driver. |
| 4 Gateway Controller | A Gateway controller is added for each Gateway device. The modules and devices configured on the Gateway are listed below the Gateway Controller and include the Gateway module, any expansion modules and the other devices attached to the module interfaces. Figure 5-1 shows an example Hardware tree with the Gateway Controllers, expansion modules and other devices.  
To add a Gateway module to the configuration, right-click on the Access GW Driver and select New Gateway Controller. |
| 5 Access Control Modules | Modules include the Gateway, Reader, Input and Output modules. Each configured module is listed under the Gateway Controller, including the Gateway module itself.  
Note The Gateway module is displayed by default. Expansion modules are displayed only if added to the configuration. For information and instructions to install modules, see the Cisco Physical Access Gateway User Guide. For instructions to configure modules, see Chapter 6, “Configuring Doors”. |
Since Gateways and related equipment are installed for specific locations, you can view door configurations in a hierarchical location map, as shown in **Figure 5-2**. This map is available in both the Hardware module and the Locations & Doors module of the Doors menu.

The location map represents doors as they are organized in the real world. For example, if an organization has a campus in Bangalore, and another in San Jose, you can create a hierarchical map for each site, and assign the door configurations to a campus, building, floor, area, or sub-area. You can name the locations as needed, and place the doors at any level of the location hierarchy.

**Figure 5-2** shows the location view in the Hardware module. Select Hierarchical Location in the View menu to display the map. Although you can modify the door configurations from this view, you cannot change the location map. See Creating the Location Map, page 5-6 for more information.

### Table 5-1 Elements of the Device Tree

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Module Interface</td>
</tr>
<tr>
<td>7</td>
<td>Devices</td>
</tr>
</tbody>
</table>

### Viewing Doors and Devices by Location

Since Gateways and related equipment are installed for specific locations, you can view door configurations in a hierarchical location map, as shown in **Figure 5-2**. This map is available in both the Hardware module and the Locations & Doors module of the Doors menu.

The location map represents doors as they are organized in the real world. For example, if an organization has a campus in Bangalore, and another in San Jose, you can create a hierarchical map for each site, and assign the door configurations to a campus, building, floor, area, or sub-area. You can name the locations as needed, and place the doors at any level of the location hierarchy.

**Figure 5-2** shows the location view in the Hardware module. Select Hierarchical Location in the View menu to display the map. Although you can modify the door configurations from this view, you cannot change the location map. See Creating the Location Map, page 5-6 for more information.

### Table 5-1 Elements of the Device Tree

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Module Interface</td>
</tr>
<tr>
<td>7</td>
<td>Devices</td>
</tr>
</tbody>
</table>

### Viewing Doors and Devices by Location

Since Gateways and related equipment are installed for specific locations, you can view door configurations in a hierarchical location map, as shown in **Figure 5-2**. This map is available in both the Hardware module and the Locations & Doors module of the Doors menu.

The location map represents doors as they are organized in the real world. For example, if an organization has a campus in Bangalore, and another in San Jose, you can create a hierarchical map for each site, and assign the door configurations to a campus, building, floor, area, or sub-area. You can name the locations as needed, and place the doors at any level of the location hierarchy.

**Figure 5-2** shows the location view in the Hardware module. Select Hierarchical Location in the View menu to display the map. Although you can modify the door configurations from this view, you cannot change the location map. See Creating the Location Map, page 5-6 for more information.

### Table 5-1 Elements of the Device Tree

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Module Interface</td>
</tr>
<tr>
<td>7</td>
<td>Devices</td>
</tr>
</tbody>
</table>

### Viewing Doors and Devices by Location

Since Gateways and related equipment are installed for specific locations, you can view door configurations in a hierarchical location map, as shown in **Figure 5-2**. This map is available in both the Hardware module and the Locations & Doors module of the Doors menu.

The location map represents doors as they are organized in the real world. For example, if an organization has a campus in Bangalore, and another in San Jose, you can create a hierarchical map for each site, and assign the door configurations to a campus, building, floor, area, or sub-area. You can name the locations as needed, and place the doors at any level of the location hierarchy.

**Figure 5-2** shows the location view in the Hardware module. Select Hierarchical Location in the View menu to display the map. Although you can modify the door configurations from this view, you cannot change the location map. See Creating the Location Map, page 5-6 for more information.

### Table 5-1 Elements of the Device Tree

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Module Interface</td>
</tr>
<tr>
<td>7</td>
<td>Devices</td>
</tr>
</tbody>
</table>
Tip

- Door configurations can be assigned to any level of the hierarchical map.
- You can drag-and-drop Gateways and Doors from one location to another.

Creating the Location Map

To create or modify the location map for door configurations, select Locations & Doors from the Doors menu. This map is also displayed in the Hierarchical Location view of the Hardware module, as described in Viewing Doors and Devices by Location, page 5-5.

Figure 5-3 shows a sample location map. You can use any combination of map elements, such as campus, building, and floor.

Use the following methods to create and modify the location map.

- To create a new base, click the **Add Base** button in the toolbar menu.
- To create a sub-location, right-click a location and select **New [Element]**.
- To change the properties for an element, right-click a location and select **Edit**.
- To add a door configuration, right-click a location and select **Add Door**. See Chapter 6, “Configuring Doors”.

You can create any combination of location elements and door configurations can be assigned to any level of the hierarchical tree. For example, if a building has only one entrance, you can assign the door configuration at the building level. For larger sites with multiple doors, you may need to assign a door configuration to a specific floor or area within the building.

Figure 5-3  Locations & Doors: Main Window

Note

Hierarchical locations cannot be deleted. Door and Gateway names must be unique.
Filtering the Devices Displayed in the Locations View

Use the View menu to select the devices or doors displayed in the Location & Doors window. For example, select Gateway Controllers to display only the Gateway Controllers in their assigned location (Figure 5-4).

**Example**

In the following example, the password is changed for all Gateways installed in a location:

**Step 1** Select **Gateway Controllers** from the View menu, as shown in Figure 5-4.

**Step 2** Right-click a location.

**Step 3** Select **Reset Gateway Password**. The passwords are reset for all Gateways assigned to that location.
Changing the Location of a Device or Door

To change the location of a door or device (including Gateways, input and output devices) from one location to another, you can drag and drop the items in the location map, or or edit the configuration, as described in the following steps.

Procedure

Step 1 Select Hardware or Locations & Doors from the Doors menu.
- Locations & Doors: Select a device or door from the View menu.
- Hardware: Select Hierarchical Location from the View menu.

Step 2 Expand the location tree to view the device or door.

Step 3 Change the location for the device or door:
- Drag and drop the device or door icon to a new location, and click Yes when the confirmation message appears.
- Select the device or door and click Edit. In the Edit window, select the Location tab and choose a new Hierarchical Location from the drop-down menu, as shown in Figure 5-5. You can also click the Choose button to select a location from the location map.

Figure 5-5 Editing the Location for a Door or Device
Viewing Device and Door Status

To view the status for a door or device use one of the options described in this section:

- Viewing a Status Summary for All Devices, page 5-9
- Viewing the Status for a Single Door, Device or Driver, page 5-10
- Monitoring Device Errors, page 5-13
- Viewing the Recent Events for a Device, Driver, or Location, page 5-14
- Generating a System Sanity Report, page 5-16

Viewing a Status Summary for All Devices

Use the Device Status module to view status information for all doors, drivers and devices.

**Step 1** Select **Device Status** from the **Doors** menu.

The Device Status window displays a status summary for all devices, as shown in Figure 5-6.

**Figure 5-6 Device Status: Main Menu**

![Device Status: Main Menu](image)

**Step 2** (Optional) Use the menu bar tools to filter or search the entries.

See **Toolbar Features**, page 3-10 for more information.

**Step 3** (Optional) Double-click an entry to view additional status details for the device, as shown in Figure 5-7.
Step 4  Click the **Extended Status** tabs to view additional details for the device. The available tabs vary depending on the device type.

---

**Viewing the Status for a Single Door, Device or Driver**

- **Step 1**  Select **Hardware** or **Locations & Doors** from the **Doors** menu.
- **Step 2**  (Optional) Use the menu bar tools to filter or search the entries.
- **Step 3**  Select a door, device or driver.

The **Status** and **Extended Status** fields appear in the right side of the window.

**Tip**  You can also right click a driver, device or location, and select **View Device Status** from the drop-down menu.
Figure 5-8 shows an example for a Gateway device in the Hardware module.

**Figure 5-8  Status and Extended Status in the Hardware Module**

**Step 4**  Click the **Extended Status** tabs to view additional details for the device.

The available tabs vary depending on the driver or device type.
Understanding Device Status Colors

The status of a Gateway, Door, or driver is signified by the color in the icon, and the color bar in the Status field, as shown in Figure 5-9.

**Figure 5-9  Device Status Colors**

<table>
<thead>
<tr>
<th>Color</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Green</td>
<td>![Green Icon]</td>
<td>The device or door is Up and the configuration is current.</td>
</tr>
<tr>
<td>2 Dark Green</td>
<td>![Dark Green Icon]</td>
<td>(Gateways only) The Gateway is Up, but has configuration changes that have not been applied (downloaded). See Applying Configuration Changes to Gateways, page 6-17.</td>
</tr>
<tr>
<td>3 Red</td>
<td>![Red Icon]</td>
<td>The device or door is in Down or Unknown state.</td>
</tr>
<tr>
<td>4 Green, Dark Green, or Red</td>
<td>![Green, Dark Green, or Red Icon]</td>
<td>The Status bar color also signifies the device or door status.</td>
</tr>
</tbody>
</table>
Monitoring Device Errors

To view a summary of the errors that occurred in the Cisco PAM system, do the following:

Step 1  Select Error Monitoring from the Admin menu.

The main window displays a summary of the errors for all devices, as shown in Figure 5-10. By default, the errors are sorted chronologically, most recent first.

Figure 5-10  Error Monitoring: Main Window

<table>
<thead>
<tr>
<th>Time</th>
<th>Level</th>
<th>Source</th>
<th>Error Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/22/2009 09:52:11</td>
<td>Error</td>
<td>COMMAND</td>
<td>Error: Send...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:53:51</td>
<td>Error</td>
<td>COMMAND</td>
<td>Required fields module type or serial number missing in modul...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:53:47</td>
<td>Error</td>
<td>DEVICECFG</td>
<td>Required fields module type or serial number missing in modul...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:53:44</td>
<td>Error</td>
<td>COMMAND</td>
<td>Error: Send...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:55:43</td>
<td>Error</td>
<td>COMMAND</td>
<td>Failed to receive response</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:50:35</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:50:09</td>
<td>ERROR</td>
<td>COMMAND</td>
<td>Failed to receive response</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:49:03</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:29:05</td>
<td>ERROR</td>
<td>COMM</td>
<td>Lost Connection With The Remote Host</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:30:45</td>
<td>ERROR</td>
<td>COMM</td>
<td>Lost Connection With The Remote Host</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:30:11</td>
<td>ERROR</td>
<td>DEVICECFG</td>
<td>Required fields module type or serial number missing in modul...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:31:31</td>
<td>ERROR</td>
<td>DEVICECFG</td>
<td>Required fields module type or serial number missing in modul...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:31:25</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 09:35:27</td>
<td>ERROR</td>
<td>COMM</td>
<td>Lost Connection With The Remote Host</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:56:18</td>
<td>ERROR</td>
<td>DEVICECFG</td>
<td>Error: (not found)</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:35:17</td>
<td>ERROR</td>
<td>DEVICECFG</td>
<td>Error: (not found)</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:35:17</td>
<td>ERROR</td>
<td>DEVICECFG</td>
<td>Error: (not found)</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:32:13</td>
<td>ERROR</td>
<td>SECURITY</td>
<td>Error: (not found)</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:20:42</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:20:36</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:20:19</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
<tr>
<td>12/22/2009 08:20:18</td>
<td>ERROR</td>
<td>COMM</td>
<td>Error in Creating A Channel: Exception: (bound closed before...</td>
<td></td>
</tr>
</tbody>
</table>

Step 2  (Optional) Use the menu bar tools to filter or search the entries.

See Toolbar Features, page 3-10 for more information.

Step 3  (Optional) Double-click an entry to view additional status details for the device, as shown in Figure 5-11.
Viewing the Recent Events for a Device, Driver, or Location

To view a list of recent events for a device or driver, do the following:

Step 1  Select Hardware or Locations & Doors from the Doors menu.

Step 2  (Optional) Use the menu bar tools to filter or search the entries. See Toolbar Features, page 3-10.

Step 3  Right-click the device or driver, and select View Recent Events from the drop-down menu, as shown in Figure 5-12.

Step 4  Double-click an event to view event details, as shown in Figure 5-13.
Figure 5-13  Recent Events

See Viewing Events, Alarms and Audit Trail Records, page 10-3 for more information.
Generating a System Sanity Report

System sanity reports provide information about potential system inconsistencies. For example, it includes a summary of doors that are administratively down, devices and doors that are disabled, and other information. Sanity reports can be viewed online, or saved to your computer in a variety of formats. Figure 5-14 shows a sample report.

Figure 5-14   System Sanity Report Example

You can also configure automated rules to automatically generate and send system sanity reports. Complete the instructions in Configuring Global I/O Automated Rules, page 11-12 and select Sanity Report Action in the Actions field.

Sanity reports include the following topics:

- Doors that are administratively down.
- Devices and doors that are disabled.
- Door templates that are not used in the system.
- Device templates that are not used in the system.
- Gateways with pending configuration changes.
- Doors not associated with any access policy.
- Doors set up with default mode Open.
- Door schedules that are not used.
• Door groups not associated with any access policy.
• Schedules that are not used.
• Workweeks, holidays, time entry collections, or time ranges that are not used.
• Access policies that are not assigned to any badge.
• Badges that are not associated with any credential template.
• Badges that are temporarily de-activated, inactive, or expired.
• Badges that are added or changed since the most recent download.
• Badges that are not assigned to any personnel record.
• Cameras that are offline.
• Gateways that are offline.
• Gateways that are set to a different time zone from the Cisco PAM.

Procedure
To view and save system sanity reports, do the following:

Step 1  Select Hardware from the Doors menu.
Step 2  Right-click the Access GW Driver and select Run System Sanity Report, as shown in Figure 5-15.

Figure 5-15  System Sanity Report Command

Step 3  In the Sanity Report window, expand the menu for a topic, as shown in Figure 5-16.
In Figure 5-16, the topic Door groups not associated with any access policy is expanded to show that the Lobby Door Group is not associated with any access policy.

**Step 4** (Optional) Open the sanity report in a separate window, or save it to your computer.

a. Click the **Report** button, as shown in Figure 5-16.

b. In the Report Generation Window (Figure 5-17), select the **Format** for the report.
c. Select the report output.
   - Open in report viewer
   - Save as document
   - Open as document

d. Select the document format from the drop-down menu (only if you chose to save or open the report as a document). For example: PDF.

e. Click OK.

f. If saving the report to a file, enter a file name, select the file location, and click Save.

---

Note

A sample sanity report is shown in Figure 5-14 on page 5-16.
Understanding Door Configurations and Templates

This section includes the following information

- Overview, page 5-20
- Sequence for Configuring Templates and Doors, page 5-21
- Door Configurations and Templates, page 5-22
- Template Types, page 5-22
- Impact of Template Changes on Configured Doors and Devices, page 5-23
- Gateway Templates, page 5-23
- Understanding Door Templates, page 5-23
- Understanding Device Templates, page 5-24
- Understanding Credential Templates, page 5-24
- Understanding Reader LED Profiles, page 5-24

Overview

Configuring an access control system for a large number of doors can be complex and time consuming. For example, if an organization has 500 doors, each door may include a different set of devices and access control rules. Some doors may include only a lock, a reader, and a REX (request to exit) device, while other doors may also include sensors and cameras. Lobby doors may need to be unlocked during business hours, while others should remain locked and require badge access at all hours. If the requirements for a door or set of doors changes, the settings must be manually entered and tracked for each door.

To manage this complexity, Cisco Physical Access Manager supports door and device templates. Templates allow you to create standard configurations that can be applied to groups of doors.

For example, if all the lobby doors in your organization use a similar set of equipment and access control rules, and all lab doors use a different set of devices and configurations, you can create one door template for lobby doors, and another for lab doors. To create a door configuration, just assign the pre-defined door template to a Gateway.

Since a door configuration references a door template, all template settings or changes to those settings are reflected by the door. You can easily override most template settings for a single door by deselecting the Default checkbox next to each field and entering a custom value. The current door setting is changed, but the template and the other doors that reference that template are unaffected.

Using templates, a campus that includes 500 doors can be categorized into 10 different door categories (such as lobby, lab, records, etc.). With Cisco PAM you create 10 different door templates instead of 500 individual door configurations. You also have full flexibility to change settings for a single door, or groups of doors.
Sequence for Configuring Templates and Doors

Figure 5-18 outlines the main tasks to create templates and apply them to door configurations.

Figure 5-18  Sequence for Configuring Templates and Doors

Device template created or edited and saved

Credential template created or edited and saved

Door template created or edited using device and credential templates

Create door using a door template

Door properties modified if desired

Final Door Configuration

Tip

See also Installation and Configuration Summary, page 1-3.
Door Configurations and Templates

Door configurations are sets of device hardware assigned to a Gateway. Door configurations usually include the following devices:

- **Lock**: Used to lock the door.
- **Rex**: REX is an abbreviation for request to exit. A REX is a type of door hardware, typically a button that allows people to exit through an access point without using a badge. Push button type REX can automatically relock the door immediately or after a delayed time interval. REX devices also include non-push button devices.
- **Reader**: A device used to read a user’s card credentials.
- **Door Sensor**: A device that senses if the door is open or closed.
- **Deadbolt**: An additional lock used for added security.
- **Door Swing**: A device used to open the door with a mechanical arm or other mechanism.

Door configurations are created by assigning door templates to a Gateway. Door templates contain pre-defined device configurations.

- **Adding Gateways and Doors Using Templates, page 6-2**: this method uses a step-by-step script that prompts you to add a Gateway to the system, create one or more door configurations, and assign a door template to each door. This is the quickest way to add a completely new set of hardware to the system.
- **Adding Doors Using Door Templates, page 6-7**: using this method, the Gateway must already be entered in the system, usually after a Discovered Configuration, or when adding an additional door configuration to an existing Gateway.

Template Types

There are five different types of templates. Each template is as a building block to provide pre-defined configurations for the next level.

- **Gateway Templates**: defines basic attributes of the Gateway module such as the time zone, support for one or two doors, the attached expansion modules, and the door templates assigned to the Gateway. Changes to a Gateway template do not impact configured Gateways (only new Gateway configurations).
- **Understanding Door Templates**: defines a set of door hardware devices and settings. Door templates are assigned to Gateway modules to simplify door configuration. Door templates also reference device templates (see below) to simplify device configuration.

<table>
<thead>
<tr>
<th>Note</th>
<th>Changes made to door, device, and credential templates also change any doors or devices configured with those templates.</th>
</tr>
</thead>
</table>

- **Understanding Device Templates**: defines typical settings for devices, such as locks and sensors. Device templates are used to help define door templates.
- **Understanding Credential Templates**: defines the card data format for a reader, including how to extract and encode the data collected from the reader or keypad.
- **Understanding Reader LED Profiles**: defines the LED states on a reader interface for a Gateway or Reader module.
Impact of Template Changes on Configured Doors and Devices

- Changes to a Gateway template do not impact configured Gateways. Only new Gateway configurations include the new settings. Gateway templates assist in new configurations only.
- Door configurations are impacted whenever the template settings for that door are changed, unless you enter a custom setting for that door.
- Changes to a door or device configuration, including changes to a template, do not take effect until the configuration is applied to the effected Gateways. See Applying Configuration Changes, page 6-17 for more information.
- Each template type includes a set of default templates. Most attributes for these default templates cannot be changed in the template. They can only be changed for an individual device. Only user-created templates can be modified.

Gateway Templates

Gateway templates include pre-defined sets of expansion modules and other devices, and basic attributes such as the time zone. To create a Gateway template, save the template from a previously configured device, as described in Creating Custom Gateway Configurations and Templates, page 7-2.

Gateway templates are used when configuring a new Gateway Controller in the Hardware module. For instructions to use Gateway templates, see Adding Gateways and Doors Using Templates, page 6-2.

Tip
To create an exact copy of a Gateway configuration for a single Gateway, see Cloning a Gateway Configuration, page 6-27.

Understanding Door Templates

Door template specify the following:

- The number and types of devices that belong to the door using this door template.
- The default properties of the door. These default properties can be overridden in the door configuration.

Door templates are assigned to a Gateway using one of the following methods:

- Adding Gateways and Doors Using Templates, page 6-2
- Adding Doors Using Door Templates, page 6-7

For example, use the Hardware module device view to configure a Gateway and then assign one or more door configurations to the Gateway. The door configurations are defined using templates.

If the basic Gateway configuration was entered using a Discovered configuration, use the Locations view to define doors using door templates or assign a door template to the door.

Tip
You can also override a template setting for a specific door or device without effecting other doors or the template settings.

To create and modify door templates, see Chapter 7, “Configuring Door and Device Templates”.

Understanding Device Templates

Device templates operate on the same concept as door templates, allowing you to create common configurations for devices, such as locks and readers.

For example, a typical access control solution might use one or two types of locks in multiple locations, with each lock type using a similar configuration. Or, the locks may use different configurations in different locations. In either case, instead of creating separate configurations for every lock in the system, you can create a device template for each type of lock that uses a similar configuration.

Device templates are applied to a specific Gateway interface, or used to define the devices in door templates. If a device requires a different configuration, you can easily override the settings for a specific device without effecting the other devices or the template.

Tip
Cisco PAM includes sample templates, or you can create new templates. There is no limit to the number of templates in a system.

Changes to a door configuration or device, including changes to a template, do not take effect until the configuration is downloaded to the effected Gateways. See Applying Configuration Changes, page 6-17 for more information.

Related Documentation

Chapter 6, “Configuring Doors”.
Chapter 7, “Configuring Door and Device Templates”.

Understanding Credential Templates

When an access control card is presented to a reader, the reader reads a set of bits. The reader needs to know how to interpret the bits, how to validate the data, and how to extract relevant card information. Credential Templates specify the card data format for a reader, and are used to configure reader device templates.

The data specification include the following:

- Card data fields and data range
- Parity bits and their bit position for data validation
- Marker bits and their bit positions/range using sentinels

Each credential template has Primary and Secondary Data fields to determine how the card data is extracted.

See Configuring Credential Templates, page 7-17 for more information.

Understanding Reader LED Profiles

Use the Reader LED module to create settings for LED lights on the reader interface of a Gateway or Reader module. The profiles are applied to reader interfaces in the Hardware module, or to door templates. See Configuring Reader LED Profiles, page 7-21 for more information.
Understanding Door Modes, Door Schedules, and the First Unlock Feature

- Overview, page 5-25
- Understanding Door Modes, page 5-26
- Viewing the Door Mode Status, page 5-27
- Understanding the Default Door Mode, page 5-28
- Understanding the Scheduled Door Mode, page 5-28
- Understanding First Unlock Impact on the Scheduled Mode, page 5-29
- Manually Override the Door Mode Using Commands, page 5-29
- Impact of Gateway Reset on the Default and Scheduled Modes, page 5-31
- Example: Configuring the Default and Scheduled Door Modes, page 5-32

Overview

Each door configuration has a default mode that defines if the door is locked, unlocked, secured, or left open. The door remains in this mode at all times unless you configure an optional schedule to define exceptions to the default mode. For example, if the default mode for a door is Lock, and you define a door schedule that automatically unlocks the door between 8 am and 5 pm. (Close), then the door will be locked at all hours except 8 am to 5 pm.

In addition, the First Unlock feature ensures that the door schedule (and associated mode) is activated only if a user successfully swipes a badge to access the door. This is useful in situations such as a snow day, when employees may not be able to reach work. The door is not automatically unlocked unless a badge holder is physically present.
To configure door modes and door schedules, use the door Properties window shown in Figure 5-19.

**Figure 5-19  Door Properties Window**

The door Properties window includes the following four fields:

- **Default mode**: the default mode of the door. The door remains in this mode at all times except when a schedule is defined. See Understanding the Default Door Mode, page 5-28.

- The **Door enable schedule**: specifies a door schedule for the times and days when a different door mode is applied. If you select a schedule, the schedule will override the default mode for the times and days defined in the schedule. See Understanding the Scheduled Door Mode, page 5-28.

- **Scheduled door mode**: the mode used when the door scheduled is applied.

- **First unlock**: determines if the schedule is activated only after the first successful badge swipe. The door remains in default mode until a badge is used to access the door, even after the beginning time for the schedule. See Understanding First Unlock Impact on the Scheduled Mode, page 5-29.

**Tip**

See Example: Configuring the Default and Scheduled Door Modes, page 5-32 to create a schedule and apply it to a door. See also See Step 6, page 7-10 in Configuring Door Templates.

**Understanding Door Modes**

A door can be in one of four door modes:

- **Open**: the door is held open and the lock is in unlocked state.
- **Close**: the door is physically closed and the lock is in unlocked state.
- **Lock**: the door is physically closed and the lock is in locked state.
- **Secure**: the door is locked and the deadbolt is applied.
The Default mode defines the door mode at all times unless overridden by a door schedule or door mode command. See Understanding the Default Door Mode, page 5-28.

A Scheduled mode overrides the default mode for the days and hours in a door schedule. For example, if the default mode is Lock, you can create a door schedule to change the mode to Close during normal business hours. The door will be locked at all times except 8 am to 5 pm, when it is physically closed but unlocked. See Understanding the Scheduled Door Mode, page 5-28.

The Override mode occurs when you manually change the door mode using a door command. The Override door commands are:

- Set Door Mode Lock
- Set Door Mode Open
- Set Door Mode Secure
- Reset Door Mode (removes the override and restores the default or scheduled mode)

If you manually override the door mode using a command, the door remains in that mode until you select another door mode command or reset the Gateway. For more information, see Manually Override the Door Mode Using Commands, page 5-29.

**Viewing the Door Mode Status**

The door mode is displayed in the Extended Status pane when you select a door in the Hardware or Locations & Doors module. In the example shown in Figure 5-20, a door’s Default mode is Open and the Current mode is Close (Scheduled). This means that the door is currently in the scheduled mode of Close, but when the schedule ends, the door will return to the default mode of Open.

Figure 5-20 also shows the door mode commands used to override the Current and Default mode. In this example, if the user selects the command Set Door Mode Lock, the door will stay in Lock mode until another door mode command is selected, or the Gateway is reset. For more information, see Manually Override the Door Mode Using Commands, page 5-29 and Impact of Gateway Reset on the Default and Scheduled Modes, page 5-31.
Understanding the Default Door Mode

The default door mode is the state of the door at all times, except when an optional schedule is applied. For example, if the default mode is Lock, the door is physically closed and the lock is applied at all times. You can override the Default door mode using a door schedule, or by selecting a door command.

Understanding the Scheduled Door Mode

Door schedules define exceptions to the default door mode during specific days and times. For example, if the default door mode is Secure, the door will be in secure mode at all times except during the days and hours defined by a door schedule. To create and apply a door schedule, do the following:

1. Create the schedule using the Schedule Manager.
2. Select the schedule in the door Properties window using the Door Enable Schedule menu.
3. Select the door mode used during the schedule using the Scheduled door mode menu.

Door schedules are optional: if a door schedule is not configured, the door remains in Default mode at all times. See Example: Configuring the Default and Scheduled Door Modes, page 5-32 for instructions to create a schedule and apply it to a door.

Door schedules change the door mode at the days and times included in the schedule. If a door is set to open every workday at 8 am, the door opens even if it is a holiday and no one is physically present. See Understanding First Unlock Impact on the Scheduled Mode, page 5-29 to avoid this situation.

To override a door schedule, see Manually Override the Door Mode Using Commands, page 5-29.
Understanding First Unlock Impact on the Scheduled Mode

First Unlock ensures that the door schedule (and associated mode) is activated only if a user successfully swipes a badge to access the door. This is useful in situations such as a snow day, when employees may not be able to reach work. The door is not automatically unlocked unless a badge holder is physically present. When the door is accessed with a valid badge, the door schedule is activated and the Scheduled Door Mode is applied. See Example: Configuring the Default and Scheduled Door Modes, page 5-32 for instructions to apply the First Unlock option.

Door Mode Changes and First Unlock

A badge is required to activate the door schedule (and associated mode) anytime the door mode is reset, after the Gateway is reset, or after a power failure to the Gateway.

Applying First Unlock

The First Unlock feature is applied immediately when a door configuration is changed. For example, if a Cisco PAM administrator changes a door configuration at 10 am to include First Unlock, the change is applied immediately and the door returns to Default mode until accessed with a badge to activate the scheduled mode.

For additional information on operating doors that are configured with First Unlock, see the following:

- Manually Override the Door Mode Using Commands, page 5-29
- Impact of Gateway Reset on the Default and Scheduled Modes, page 5-31

Manually Override the Door Mode Using Commands

When the door mode is manually changed using a door command, the current mode is displayed as Override. Door remain in the Override mode until another door command is selected, or the Gateway is reset.

For example, in Figure 5-21 the current mode is Close (Scheduled). Right click the door and select Set Door Mode Lock. The current mode is changed to Lock (Override), as shown in Figure 5-22 on page 5-31.
The current mode remains Lock (Override) until you do one of the following:

- Select another door mode command. For example, **Set Door Mode Open**.
- Select the **Reset Door Mode** command to remove the override and restore the configured default and scheduled modes. If a door schedule is configured, and the time is within the schedule, the door enters the scheduled mode immediately (however, if First Unlock is configured, the scheduled mode is not activated until the door is accessed with a badge).
- Reset the Gateway, as described in **Impact of Gateway Reset on the Default and Scheduled Modes**, page 5-31. Resetting the Gateway has the same affect as the **Reset Door Mode** command.

For example, in Figure 5-22 the current door mode is Lock (Override). The door stays in the override mode until you select another door mode or reset the Gateway. In this example, the **Reset Door Mode** command is selected, which returns the door to the scheduled mode. However, since the First Unlock feature is configured, the door stays in Default mode (Open) until the door is accessed with a valid badge.
Impact of Gateway Reset on the Default and Scheduled Modes

When a Gateway is reset, the default mode, door schedule, and First Unlock rule are reapplied. This has the same effect as invoking the **Reset Door Mode** command, as described in [Manually Override the Door Mode Using Commands](#).

The Gateway is reset using the **Reset Gateway** command, or when the Gateway power is turned off and on.

**Example 1**

- The default door mode is **Lock** (physically closed and locked).
- The scheduled door mode from 8 am to noon is **Close** (physically closed and unlocked).
- First Unlock is set to **Yes**.

If power to the Gateway goes off and comes back on at 9 am (during the scheduled mode), the Gateway is reset. Since First Unlock is configured, and the door returns to the default state (Lock) until a badge is swiped to reactive the scheduled door mode (Close).

**Example 2**

- The default door mode is **Lock** (physically closed and locked).
- The scheduled door mode from 8 am to 5 pm is **Close** (physically closed and unlocked).
- At 3 pm, the guard manually sets the door to Lock mode and goes to break (see [Manually Override the Door Mode Using Commands](#), page 5-29).
- First Unlock is set to **No**.
While the guard is away, another user invokes the Reset Gateway command in Cisco PAM. Since the First Unlock feature is not configured, the scheduled mode is immediately applied and the door is placed in Close (physically closed and unlocked). The door is now unlocked even though the guard is absent.

Example: Configuring the Default and Scheduled Door Modes

In the following example, a door schedule is created for a lobby door. The door should be physically closed but unlocked and open to the public during normal working hours, from 8 am to 5 pm. However, the door should also be locked from 12 noon until 1 pm when the receptionist is at lunch. Since this location occasionally suffers snow storms that close roads and delay traffic, we want to keep the door locked in the morning until the receptionist (or another employee) arrives and accesses the door with a badge, even if they arrive after the scheduled unlock time of 8 am. (the door should not automatically unlock for public access at 8 am, even if there is no employee on-site). This First Unlock rule is also applied to the lunch hour, so the door remains locked at 1 pm until the receptionist or another badge holder physically accessed the door.

Note

The following sample schedule does not include exceptions for holidays or other special cases. For complete instructions to configure door schedules, see Using the Schedule Manager, page 9-7.
Understanding Door Modes, Door Schedules, and the First Unlock Feature

Chapter 5  Understanding Door Configuration

To do this

Use this display

**Step 1**

Create a schedule for the door.

**Note**  Create door schedules that define the times the door is not in default mode.

- a. Select **Schedules** from the Doors menu, in the Schedule Manager sub-menu.
- b. Click **Add**.
- c. Enter the name and description for the schedule.
- d. For **Schedule Type** select **Door Policy** (only door policy schedules appear in door configurations).
- e. For **Type**, select **Work Weeks**. From the **Values** menu, select **Default Work Weeks** (Monday - Friday)
- f. For **Action**, select **Use Schedule Mode**.
- g. Create a custom **Time Range** for the schedule (for example: “8-5, minus lunch”):
  - For **Time Ranges** click **New**.
  - In the Time Ranges window, enter a Name and Description for the time range.
  - Enter a start time of 8:00 and end time of 12:00, and click **Add** to add the entry in the list box.
  - Enter a start time of 13:00 (1 pm) and an end time of 17:00 (5 pm), and click **Add**.
  - **Click Save and Close**.
- h. In the Add Schedule window, select the new range **(8-5, minus lunch)** from the **Time Range** menu.
- i. Click **Add** to add the schedule to the list.
- j. **Click Save and Close** to create the door schedule. The door schedule appears in the Schedules window.

**Note**  The schedule is not active until you apply it to a door, as described in the following steps.
Understanding Door Modes, Door Schedules, and the First Unlock Feature

Chapter 5  Understanding Door Configuration

To do this

Step 2  Open the door configuration Properties window.

  a.  Select Hardware or Locations and Doors from the Doors menu.

  b.  Double click an existing door icon to open the door edit window.

  c.  Select Properties.

**Tip**  To create or modify a door template with these settings, select Door Templates from the Doors menu, in the Templates sub-menu. See Configuring Door Templates, page 7-7.

Step 3  Apply the door mode and schedule settings.

The following example places the door in Lock mode at all times, except for Monday to Friday, 8 am to 12 pm, and 1 pm to 5 pm, when the door is in Close mode.

**Tip**  To override the default template settings, uncheck the box in the right column to activate the field.

  a.  For Default mode, select Lock. The door is physically closed and the lock applied at all hours by default. A badge is required for access.

  b.  For Door enable schedule, select 8-5, minus lunch. This is the schedule created in Step 1.

  c.  For Scheduled door mode, select Close. The door is physically closed during the door schedule hours, but the lock is not applied.

  d.  For First Unlock, select Yes. The door remains in Lock mode in the morning and after lunch break until a badge holder physically swipes their badge to activate the schedule and place the door in Close mode.

  e.  Click Save and Close to save the changes.
### Chapter 5  Understanding Door Configuration

#### Understanding Door Modes, Door Schedules, and the First Unlock Feature

**Step 4**

**To do this**  
Apply the door configuration changes.  
Right-click a location or Gateway and select **Apply Configuration Changes**.

**Note**  
Gateways must be in the Up state, signified by a green triangle in the icon. A dark green triangle means configuration changes that have not been applied.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the door configuration changes.</td>
<td><img src="image" alt="Cisco Physical Access Manager Interface" /></td>
</tr>
</tbody>
</table>

[![Gateway Interface](image)](image)
Locating Serial Numbers

- Locating Gateway and Expansion Module Serial Numbers
- Displaying the Cisco PAM Appliance Serial Number

Locating Gateway and Expansion Module Serial Numbers

Serial numbers for the Gateway and other expansion modules are available at the following locations:
- Printed on the back label of the module case.
- Listed in the Cisco PAM Gateway Controller properties. Open the Hardware module device view, right-click on the module, select Edit and then Properties.

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 2-4.
- 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 2-2, 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 Status, as shown in Figure 5-23.

**Step 3** Refer to the entry for Serial Number.

*Figure 5-23 Cisco PAM Appliance Serial Number*
Related Documentation

- Chapter 6, “Configuring Doors”
- Chapter 7, “Configuring Door and Device Templates”.
- To install Gateways and expansion modules, see Cisco Physical Access Gateway User Guide.