Cisco Physical Access Manager User Guide
Release 1.2.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-20930-02
CONTENTS

Preface xiii

Obtaining Documentation and Submitting a Service Request xiii

Safety Warnings xiii

Safety Guidelines xvi

General Precautions xvi

Protecting Against Electrostatic Discharge xvii

Rack Installation Safety Guidelines xvii

Overview 1-1

Contents 1-1

Overview 1-2

Installation and Configuration Summary 1-3

Install the Hardware and Software Components 1-3

Configure Doors and Users in Cisco PAM 1-4

User Guide Contents 1-9

Cisco PAM Software Overview 1-11

Cisco PAM Desktop Client Software 1-11

Cisco PAM Server Administration Utility 1-12

Cisco Physical Access Gateway Administration Utility 1-13

The Enterprise Data Integration (EDI) Desktop Studio 1-14

Cisco Video Surveillance Viewer 1-15

Badge Designer 1-15

Configuring and Monitoring the Cisco PAM Server 2-1

Contents 2-1

About the Cisco PAM Server Administration Utility 2-2

Logging on to the Cisco PAM Server Administration Utility 2-2

Using Redundant Appliances for High Availability 2-2

Understanding IP Addresses on the Cisco PAM Server 2-3

Cisco PAM Appliance IP Address 2-3

Gateway Module IP Addresses 2-3

Entering the Initial Server Configuration 2-4

Before You Begin 2-4
## Contents

- Connecting a PC to the Appliance 2-4
- Initial Setup Instructions 2-5
- Performing Additional Configuration, Administration, and Monitoring Tasks 2-12
- Understanding the Cisco PAM Server Username and Password 2-16
  - Changing the Cisco PAM Server Administration Utility Password 2-17
  - Resetting a Forgotten Password 2-18
    - Enabling the **Forgot Password** Feature 2-19
    - Recovering a Lost Server Password 2-20
- Obtaining and Installing Optional Feature Licenses 2-21
  - Understanding Module Licenses 2-21
  - Licenses in a Redundant Configuration 2-22
  - Purchasing Additional Feature Licenses 2-22
    - Part Numbers for the Optional Feature Licenses 2-22
- Installing Additional Licenses 2-23
  - Option 1: Enter the Product Authorization Key to Download the License File 2-23
  - Option 2: Obtain the License File from the Cisco Web Site 2-24
- Displaying a Summary of Installed Licenses 2-25
  - Displaying the Cisco PAM Appliance Serial Number 2-25
- Performing a Graceful Failover with Redundant Appliances 2-26
- Troubleshooting and Monitoring 2-26
- Next Steps 2-27

### CHAPTER 3

**Getting Started With the Cisco PAM Desktop Software** 3-1

- Contents 3-1
- Before You Begin 3-2
- Installing or Updating the Cisco PAM Desktop Software 3-2
- Logging in to Cisco PAM 3-3
- Understanding the Start Page and Window Management 3-4
- Keeping a Module On Top 3-6
  - Choosing Multiple *Always on Top* Windows 3-7
  - Deselecting *Always on Top* 3-7
- User Interface Elements 3-8
- Toolbar Features 3-10
  - Creating Reports 3-10
  - Using Filters 3-12
    - Filter Example 3-12
  - Revising the Column Display 3-14
  - Using Group Edit 3-14
## Configuring User Access for the Cisco PAM Desktop Client

### Contents
- Defining User Profiles for Desktop Application Access 4-2
- Creating User Login Accounts and Assigning Profiles 4-8
- Configuring LDAP User Authentication 4-11
  - Configure the LDAP Server 4-11
    - LDAP Example: User Principal Name 4-12
    - LDAP Example: sAMAccountName 4-13
  - Create the LDAP User Account in Cisco PAM 4-13
- Viewing Audit Records for Changes to Usernames 4-15
- Managing Desktop Client Passwords 4-16
  - Changing Your Password 4-16
  - Changing Another User’s Password 4-16
  - Managing the c pamadmin Login and Password 4-17

## Understanding Door Configuration

### Contents
- Provisioned (Pre-Populated) vs. Discovered Gateway Configurations 5-2
  - Provisioned (Pre-Populated) Configuration 5-2
  - Discovered Configuration 5-2
- Viewing Device and Door Configuration 5-3
  - Viewing Doors and Devices in the Hardware View 5-3
  - Viewing Doors and Devices by Location 5-5
    - Creating the Location Map 5-6
    - Filtering the Devices Displayed in the Locations View 5-7
    - Changing the Location of a Device or Door 5-8
- Viewing Device and Door Status 5-9
  - Viewing a Status Summary for All Devices 5-9
  - Viewing the Status for a Single Door, Device or Driver 5-10
- Understanding Device Status Colors 5-12
- Monitoring Device Errors 5-13
- Viewing the Recent Events for a Device, Driver, or Location 5-14
- Generating a System Sanity Report 5-16
- Understanding Door Configurations and Templates 5-20
  - Overview 5-20
### Sequence for Configuring Templates and Doors 5-21

- **Door Configurations and Templates** 5-22
  - **Template Types** 5-22
  - **Gateway Templates** 5-23
  - **Understanding Door Templates** 5-23
  - **Understanding Device Templates** 5-24
  - **Understanding Credential Templates** 5-24
  - **Understanding Reader LED Profiles** 5-24

- **Impact of Template Changes on Configured Doors and Devices** 5-23

### Understanding Door Modes, Door Schedules, and the First Unlock Feature 5-25

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

### Locating Serial Numbers 5-36
- **Locating Gateway and Expansion Module Serial Numbers** 5-36
- **Displaying the Cisco PAM Appliance Serial Number** 5-36

### Related Documentation 5-37

### Configuring Doors 6-1

- **Contents** 6-1

#### Configuring Doors 6-2

- **Adding Gateways and Doors Using Templates** 6-2
- **Adding Doors Using Door Templates** 6-7

#### Modifying Door Configurations 6-14

- **Modifying Door and Device Templates** 6-14
- **Modifying Devices in the Hardware Device View** 6-14
- **Modifying Devices in Hardware Location View** 6-15
- **Modifying Devices in the Locations & Doors Module** 6-16

#### Applying Configuration Changes 6-17

- **Applying Configuration Changes to Gateways** 6-17
- **Applying Configuration Changes in the Hardware Module** 6-17
- **Applying Configuration Changes in the Locations & Doors Module** 6-18
- **Configuration Management in Provisioned vs. Discovered Configurations** 6-18
### Contents

#### Chapter 6: Device and Gateway Configuration

- Disabling or Deleting a Device or Door  6-19
  - Disabling a Device or Door  6-19
  - Deleting Devices and Doors  6-20
    - Enabling the Delete Options  6-21
    - Deleting a Device  6-22
    - Deleting a Gateway Controller  6-22
- Enabling a Device or Door  6-23
  - Disable and Enable a Device and Door: Example  6-23
- Cloning a Gateway Configuration  6-27
- Configuring Device Groups  6-28
- Replacing a Gateway or Expansion Module  6-31
- Changing Gateway Passwords  6-31
- Device and Driver Commands in the Hardware Device View  6-34
  - Access GW Driver Commands  6-34
  - Gateway Controller Commands  6-35
  - Reader Module Commands  6-37
  - Input and Output Module Commands  6-37
  - Logical Driver Commands  6-38
- Door Modes and Commands  6-39
  - Door Modes  6-39
  - Door Commands  6-39

#### Chapter 7: Configuring Door and Device Templates

**Contents**  7-1

- Creating Custom Gateway Configurations and Templates  7-2
- Configuring Door Templates  7-7
- Configuring Device Templates  7-14
  - Creating a Device Template  7-15
- Configuring Credential Templates  7-17
  - Overview  7-17
    - Credential Templates Settings Summary  7-18
      - Wiegand Keypad  7-18
      - Keypad  7-18
    - Creating a Credential Template  7-19
- Configuring Reader LED Profiles  7-21
  - Configuring Reader LED and Buzzer Profiles  7-22
- Duplicating Templates  7-23
CHAPTER 8
Configuring Personnel and Badges 8-1
Contents 8-1
Configuring Personnel 8-2
Downloading Credential Changes to the Gateway Modules 8-10
Viewing Audit Records and Events for Personnel Records 8-11
  Viewing Audit Records 8-11
  Viewing Recent Events 8-13
Editing Organization and Department Lists 8-13
Importing Personnel Records Using a Comma Separated Value (CSV) File 8-15
Configuring Badges 8-20
  Configuring Badge Templates 8-20
  Badge Properties 8-22
    Badges Module: General 8-22
    Badges Module: Cisco Access Policy 8-24
    Badges Module: Advanced Gateway 8-25
    Badges Module: HSPD-12 Badge Extension 8-26
    Badges Module: Audit Records 8-27
    Badges Module: Recent Events 8-27
Using the Badge Designer 8-28
Printing Badges 8-35
  Printing Individual Badges 8-35
  Printing Multiple Badges 8-36
  Printing High Resolution Images 8-40
  Changing the Default Badge Printer 8-40
  System Configuration Settings for Badge Printing 8-41
Setting Up Image and Signature Options for Personnel Records 8-44
  Enabling Image Capture Devices 8-44
  Enabling Signature Capture Devices 8-45

CHAPTER 9
Configuring Cisco Access Policies 9-1
Contents 9-1
Configuring Access Policies 9-2
Managing Door Access With Access Control Policies 9-4
CHAPTER 10
Configuring Automated Tasks 11-1

Contents 11-1
Creating Quick Launch Buttons 11-2
Creating a Button 11-2
Creating a Button That Runs An Automated Rule 11-7
Creating Panels (Windows) of Related Buttons 11-7
Restricting User Access to Button Panels 11-8
Configuring Device Automated Rules 11-9
Configuring Global I/O Automated Rules 11-12
Enabling the Automation Driver 11-12
Configuring Automated Tasks Using Global I/O 11-14
Understanding Automated Rule Actions 11-17
Example: Automated Weekly Report 11-21
Defining Reports (Report Manager) 11-25
Using the Report Manager 11-26
Filter-based Report Template 11-27
Object SQL-based Report Template 11-28
SQL-Based Report Template 11-29

CHAPTER 11
System Integration 12-1

Contents 12-1
Contents

CHAPTER 12
Configuring URL Actions  12-2
  Creating or Modifying URL Actions  12-3
  Creating Automated Rules for URL Actions  12-7
Viewing URL Events, Alarms, and Logs  12-10
  Viewing URL Action Events  12-10
  Viewing Alarms for Failed URL Action  12-11
  Event and Alarm Response Codes for URL Actions  12-11
  Viewing Logs for URL Action Output  12-12
URL Action Failure Due to Invalid Security Certificate  12-13

Synchronizing Data Using Enterprise Data Integration (EDI)  12-14
  Before You Begin  12-14
  Installing the EDI Licence and Desktop Application  12-15
  Creating Active Directory Database Integration Projects Using EDI Studio  12-17
  Creating SQL and Oracle Database Integration Projects Using EDI Studio  12-26
  Importing, Starting, and Monitoring EDI Projects in Cisco PAM  12-33
    Importing and Starting EDI Projects  12-33
    Verifying EDI Projects (EDI Monitoring)  12-35
    Modifying a Running EDI Project  12-37
    Restarting a Failed EDI Project  12-39
    Summary of EDI Administration Functions  12-39

Accessing the SQL Database  12-41
  Personnel  12-41
  Time and Attendance  12-42
  User Tracking  12-43

CHAPTER 13
Video Monitoring  13-1

Contents  13-1
Enabling Video Monitoring  13-3
  Configuring the Camera Driver  13-3
  Associating Cameras with Doors and Devices  13-6
  PC Workstation Requirements for Live Video Viewing  13-7
  Installing the Cisco VSOM Video Client Desktop Application  13-8

Viewing Video  13-9
  Viewing Live Video in a Grid Arrangement  13-9
  Viewing Video for an Event  13-12
Defining the Duration of Event Video Recording  13-15
Managing the Camera Inventory  13-16
  Updating the Camera Inventory  13-16
  Deleting the Cisco VSM Cameras  13-18
Deleting Individual Cameras 13-22
Recording Motion Events from Cisco VSM Cameras 13-24

CHAPTER 14
System Configuration Settings 14-1
Contents 14-1
LDAP Settings 14-3
Password Policy Settings 14-5
Event/Alarms Settings 14-6
Data Entry/Validation - Personnel Settings 14-7
Data Entry/Validation - Badge Settings 14-8
Custom Personnel Fields Settings 14-10
Custom Device Fields Settings 14-11
Custom Badge Fields 14-12
Personnel ID Number Generator 14-13
PIN Generator 14-14
Card Number Generator 14-15
Support Contact Information 14-16
Badge Design 14-17
Miscellaneous Settings 14-18
Cisco Settings 14-20

APPENDIX A
Backing Up and Restoring Data A-1
Contents A-1
Backing up the Cisco PAM Database A-2
Archiving the Historical Events Database A-4
Restoring a Server Backup File A-6

APPENDIX B
Upgrading Software and Firmware B-1
Contents B-1
Upgrade Notes for Release 1.2.0 B-2
Credential Download Frequency Must be 60 Minutes or Higher B-2
The Door Groups Feature Added to Device Groups B-2
Enabling the Password Recovery Feature B-2
Upgrading From Release 1.0.3 to Release 1.2.0 B-3
Split Holiday Schedule Configurations By Month B-3
Select the Following Options When Upgrading Gateway Firmware B-3
Generic Output Devices Installed Prior to Release 1.1.0 Must Be Rewired B-3
Preface

- Obtaining Documentation and Submitting a Service Request, page xiii
- Safety Warnings, page xiii
- Safety Guidelines, page xvi

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Safety Warnings

Before you install the device, observe the safety warnings in this section.

⚠️ **Warning**

Read the installation instructions before connecting the system to the power source. Statement 1004

⚠️ **Warning**

Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord. Statement 1

⚠️ **Warning**

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units. Statement 12

⚠️ **Warning**

This unit might have more than one power cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit. Statement 106
Warning: This is a Class A Information Product, when used in residential environment, it may cause radio frequency interference, under such circumstances, the user may be requested to take appropriate countermeasures. Statement 257

Warning: Do not attempt to make such connections yourself. Contact the appropriate electric inspection authority or electrician as appropriate. Statement 285

Warning: Do not work on the system or connect or disconnect cables during periods of lightning activity. Statement 1001

Warning: To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

Warning: This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

Warning: When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

Warning: If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack. Statement 1006

Warning: There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions. Statement 1015

Warning: This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. Statement 1017

Warning: This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

Warning: This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028
Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029

Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030

Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040

Before opening the unit, disconnect the telephone-network cables to avoid contact with telephone-network voltages. Statement 1041

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations. Statement 1045

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 35° C

This equipment is intended to be grounded to comply with emission and immunity requirements. Ensure that the switch functional ground lug is connected to earth ground during normal use. Statement 1064

Installation of the equipment must comply with local and national electrical codes. Statement 1074
Safety Guidelines

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the precautions in this section.

General Precautions

Observe the following general precautions for using and working with your system:

- Observe and follow service markings. Do not service any Cisco product except as explained in your system documentation. Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock. Components inside these compartments should be serviced only by an authorized service technician.

- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your authorized service provider:
  - The power cable or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.

- Keep your system components away from radiators and heat sources. Also, do not block cooling vents.

- Do not spill food or liquids on your system components, and never operate the product in a wet environment.

- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.

- Use the product only with other Cisco-approved equipment.

- Allow the product to cool before removing covers or touching internal components.

- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service representative or local power company.

- Use only approved power cables. If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product’s electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.

- To help prevent electric shock, plug the system components and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable.

- Observe power strip ratings. Make sure that the total ampere rating of all products plugged into the power strip does not exceed 80 percent of the power strip ampere ratings limit.

- Do not use appliance or voltage converters or kits sold for appliances with your product.

- To help protect your system components from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
Position cables and power cords carefully; route cables and the power cord and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your system components’ cables or power cord.

Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local or national wiring rules.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside the device. To prevent static damage, discharge static electricity from your body before you touch any of your system’s electronic components. You can do so by touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

Rack Installation Safety Guidelines

Before installing your device in a rack, review the following guidelines:

- Two or more people are required to install the device in a rack.
- Ensure that the room air temperature is below 95°F (35°C).
- Do not block any air vents; usually 6 inches (15 cm) of space provides proper airflow.
- Plan the device installation starting from the bottom of the rack.
- Install the heaviest device in the bottom of the rack.
- Do not extend more than one device out of the rack at the same time.
- Remove the rack doors and side panels to provide easier access during installation.
- Connect the device to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack.
- Do not place any object weighing more than 110 lb. (50 kg) on top of rack-mounted devices.
Overview

This user guide describes how to install and configure the Cisco Physical Access Manager appliance using the Cisco PAM desktop software.

This chapter provides an overview of the main hardware and software components of the Cisco PAM appliance, and a summary of the chapters and topics included in this guide.

Contents

- Overview, page 1-2
- Installation and Configuration Summary, page 1-3
- User Guide Contents, page 1-9
- Cisco PAM Software Overview, page 1-11
Overview

The Cisco Physical Access Manager appliance (Cisco PAM) is a hardware and software solution that provides advanced configuration and management of the Cisco Physical Access Control system, as shown in Figure 1-1.

Figure 1-1  Cisco Physical Access Control System

The Cisco PAM desktop client is used to define access control rules, enroll users, manage badges, and configure the Cisco Physical Access Gateways modules, among other tasks.

- See User Guide Contents, page 1-9 for descriptions of the topics covered in each chapter of this guide.
- See Installation and Configuration Summary, page 1-3 for a description of the primary access control configuration tasks.
- See the Cisco Physical Access Gateway User Guide for instructions to install and configure Gateways and door-related hardware.
Installation and Configuration Summary

Complete the following tasks to install and configure your Cisco Access Control system.

- Install the Hardware and Software Components
- Configure Doors and Users in Cisco PAM

Install the Hardware and Software Components

**Step 1** Install the Server hardware. See *Cisco Physical Security Multi Services Platform User Guide* or *Cisco Physical Access 1125 Appliance User Guide* for more information.

**Step 2** Install and configure the server software. See Chapter 2, “Configuring and Monitoring the Cisco PAM Server”

**Step 3** Install the desktop client. See Chapter 3, “Getting Started With the Cisco PAM Desktop Software”

**Step 4** Install the door devices, including locks, readers and other input and output devices.

**Step 5** Install the Gateway modules and optional expansion modules, as described in *Cisco Physical Access Gateway User Guide* and the *Cisco Physical Access Gateway Quick Start Guide*.

**Note**

To ensure proper operation, test all door devices and modules on a lab bench before actual installation.

**Step 6** Enter the Gateway module’s network settings by connecting an Ethernet cable from a PC to the ETH1 interface on the Gateway module. See “Configuring and Managing the Gateway Using a Direct Connection” in the *Cisco Physical Access Gateway User Guide*. Also see the *Cisco Physical Access Gateway Quick Start Guide*.

**Step 7** Connect an Ethernet cable from the Gateway ETH0 interface to the network.

**Tip**

You can also add the Gateways to the network after configuring doors and users in Cisco PAM, as described in Configure Doors and Users in Cisco PAM, page 1-4. For more information, see Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2.
Step 8  Wait for the Gateway to connect to the Cisco PAM appliance. Verify that the Gateway status is **Up** in the Hardware view (select **Hardware** from the **Doors** menu in Cisco PAM).

### Configure Doors and Users in Cisco PAM

Configure users, doors, badges and access policies, as described in the following summary:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Assign the appropriate credential templates to the reader templates.</td>
<td><img src="image" alt="Device Templates - Cisco Physical Access Manager" /></td>
</tr>
</tbody>
</table>

**Menu:**
- Doors:Templates:Device Templates

**Instructions:**
- Understanding Device Templates, page 5-24
- Understanding Credential Templates, page 5-24
- Configuring Device Templates, page 7-14
- To create additional credential templates, see Configuring Credential Templates, page 7-17.
### Step 2

Configure Gateways and doors:

a. Use Gateway templates to add new Gateways on the Hardware menu.

b. Create the hierarchical location map (select Locations & Doors in the Doors menu).

c. Use door templates to add doors to the locations.

**Note** In this example, Gateways are configured before connecting them to the network. You can also connect the modules to the network first, and then complete the Cisco PAM configuration. See Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2 for more information.

**Menu:**
- Doors:Locations & Doors
- Doors:Hardware

**Overview Information:**
- Viewing Doors and Devices by Location, page 5-5
- Gateway Templates, page 5-23

**Instructions:**
- Creating the Location Map, page 5-6
- Adding Gateways and Doors Using Templates, page 6-2
- Adding Doors Using Door Templates, page 6-7

**Tip** To create additional Gateway and door templates, see Chapter 7, “Configuring Door and Device Templates”.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure Gateways and doors:</td>
</tr>
<tr>
<td>a. Use Gateway templates to add new Gateways on the Hardware menu.</td>
<td><img src="image1" alt="Gateway Templates" /></td>
</tr>
<tr>
<td>b. Create the hierarchical location map (select Locations &amp; Doors in the Doors menu).</td>
<td><img src="image2" alt="Location Map" /></td>
</tr>
<tr>
<td>c. Use door templates to add doors to the locations.</td>
<td><img src="image3" alt="Door Templates" /></td>
</tr>
</tbody>
</table>

**Menu:**
- Doors:Locations & Doors
- Doors:Hardware

**Overview Information:**
- Viewing Doors and Devices by Location, page 5-5
- Gateway Templates, page 5-23

**Instructions:**
- Creating the Location Map, page 5-6
- Adding Gateways and Doors Using Templates, page 6-2
- Adding Doors Using Door Templates, page 6-7

**Tip** To create additional Gateway and door templates, see Chapter 7, “Configuring Door and Device Templates”.
### Step 3
Create access policies to define the days and times users can access doors.

**Menu:**
Doors: Access Policies

**Configuration Instructions:**
Chapter 9, “Configuring Cisco Access Policies”

### Step 4
Add personnel records and assign badges to grant user access to the doors. Assign the appropriate access policies (created in the previous step) to the badge.

**Menu:**
- Users: Personnel

**Configuration Instructions:**
- Chapter 8, “Configuring Personnel and Badges”
Chapter 1  Overview

Installation and Configuration Summary

To do this | Use this display
--- | ---
**Step 5** Add the Gateway modules to the network:  
  a. Connect an Ethernet cable from a PC to the ETH1 interface on the Gateway module.  
  b. Enter the Gateway module’s network settings.  
  c. Connect an Ethernet cable from the ETH0 interface on the Gateway module to the network.  
  • Wait for the Gateway to connect to the Cisco PAM appliance. Verify that the Gateway status is *Up* in the Hardware view (select **Hardware** from the Doors menu in Cisco PAM).

Tip  The Gateways were added to the Cisco PAM configuration in **Step 2**. You can also add the Gateways to the network before configuring doors and users in Cisco PAM. See Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2 for more information.

Instructions:  
• “Configuring and Managing the Gateway Using a Direct Connection” in the *Cisco Physical Access Gateway User Guide*.

**Step 6** Apply configuration changes to the Gateway modules. Changes are not active until applied.

Menu:  
• Doors:Locations & Doors  
• Doors:Hardware

Configuration Instructions:  
• Applying Configuration Changes, page 6-17
### Step 7

(Optional) Clone the new Gateway and door configuration and apply it to another Gateway. This quickly adds an additional door to the Cisco PAM configuration. Enter the serial number and door name for the new Gateway module. Repeat this process as many times as necessary.

**Tip** You can also create a Gateway template from the configuration.

#### Menu:
Doors: Hardware

#### Configuration Instructions:
- Cloning a Gateway Configuration, page 6-27
- Creating Custom Gateway Configurations and Templates, page 7-2

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone the new Gateway and door configuration and apply it to another Gateway. Enter the serial number and door name for the new Gateway module. Repeat this process as many times as necessary.</td>
<td><img src="image" alt="Clone Gateway" /></td>
</tr>
</tbody>
</table>

**Tip** You can also create a Gateway template from the configuration.
User Guide Contents

This User Guide describes how to install and configure the Cisco PAM appliance, and how to use the Cisco PAM desktop client to configure, manage, and monitor the Cisco Physical Access Control system. Table 1-1 describes the chapters and subjects included in this guide.

Table 1-1  Chapters and Features in the Cisco Physical Access Manager User Guide

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Overview”</td>
<td>Introduces the main Cisco PAM hardware and software components.</td>
</tr>
<tr>
<td>Chapter 2, “Configuring and Monitoring the Cisco PAM Server”</td>
<td>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.</td>
</tr>
<tr>
<td>Chapter 3, “Getting Started With the Cisco PAM Desktop Software”</td>
<td>Describes how to install the Cisco PAM desktop client software, log on to Cisco PAM, and begin configuring access control features and doors. This chapter also includes an overview of the Cisco PAM user interface.</td>
</tr>
<tr>
<td>Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client”</td>
<td>Describes how to configure Cisco PAM operators.</td>
</tr>
<tr>
<td>Chapter 5, “Understanding Door Configuration”</td>
<td>Describes the terms and concepts used to configure doors and templates.</td>
</tr>
<tr>
<td>Chapter 6, “Configuring Doors”</td>
<td>Describes how to configure doors, including how to clone Gateway configurations to quickly create another door.</td>
</tr>
<tr>
<td>Chapter 7, “Configuring Door and Device Templates”</td>
<td>Describes how to create and modify Cisco PAM door and device templates.</td>
</tr>
<tr>
<td>Chapter 8, “Configuring Personnel and Badges”</td>
<td>Describes how to create the personnel records and badges used to access doors in the Cisco Physical Access Control system.</td>
</tr>
<tr>
<td>Chapter 9, “Configuring Cisco Access Policies”</td>
<td>Describes how to create the Access Policies assigned to badge holders that define which doors they can access, and the dates and times of that access. Once created, access policies are assigned to personnel badges.</td>
</tr>
<tr>
<td>Chapter 10, “Events &amp; Alarms”</td>
<td>Describes how to view the event and alarm records in Cisco PAM, and how to use the Event Policy Manager to configure the log codes and other properties that define how events are captured and managed.</td>
</tr>
<tr>
<td>Chapter 11, “Configuring Automated Tasks”</td>
<td>Describes how to used to create and manage automated tasks to perform actions such as Trigger a relay when an alarm is generated, play alarm video, or generate a report and e-mail it to a user.</td>
</tr>
<tr>
<td>Chapter 12, “System Integration”</td>
<td>Describes how to use EDI to automatically synchronize Cisco PAM records with the databases from other sources, such as an organization’s HR personnel records. Also describes how to use URL Actions to automatically synchronize data with other sources.</td>
</tr>
<tr>
<td>Chapter 13, “Video Monitoring”</td>
<td>Describes how to view live and recorded video streams from the Cisco Video Surveillance Manager (Cisco VSM), including how to view video clips associated with events and alarms.</td>
</tr>
<tr>
<td>Chapter 14, “System Configuration Settings”</td>
<td>Describes the system-wide site settings available in the System Configuration module.</td>
</tr>
</tbody>
</table>
Table 1-1  Chapters and Features in the Cisco Physical Access Manager User Guide

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A, “Backing Up and Restoring Data”</td>
<td>Describes how to backup and restore the Cisco PAM database.</td>
</tr>
<tr>
<td>Appendix B, “Upgrading Software and Firmware”</td>
<td>Describes how to upgrade or reinstall the Cisco PAM server software, desktop client software, and Gateway module firmware.</td>
</tr>
<tr>
<td>Appendix C, “Troubleshooting”</td>
<td>Describes troubleshooting techniques for the Cisco PAM software.</td>
</tr>
<tr>
<td>Appendix D, “Security”</td>
<td>Provides security information related to the configuration and operation of the Cisco PAM software.</td>
</tr>
<tr>
<td>Glossary</td>
<td>Provides definitions to terms used in the Cisco PAM system.</td>
</tr>
</tbody>
</table>
Cisco PAM Software Overview

Although the Cisco PAM desktop client is the main tool used to configure and manage the Cisco Physical Access Control system, a number of additional utilities perform specific tasks, such as configuring the appliance or designing data integration projects.

- Cisco PAM Desktop Client Software, page 1-11
- Cisco PAM Server Administration Utility, page 1-12
- Cisco Physical Access Gateway Administration Utility, page 1-13
- The Enterprise Data Integration (EDI) Desktop Studio, page 1-14
- Cisco Video Surveillance Viewer, page 1-15
- Badge Designer, page 1-15

Cisco PAM Desktop Client Software

The Cisco Physical Access Manager (Figure 1-2) is a Java-based desktop client used to configure the Cisco PAM appliance and access control features.

See Chapter 3, “Getting Started With the Cisco PAM Desktop Software” for instructions to install the application and log in to the system. This chapter also includes an introduction to the Cisco PAM appliance user interface, and a summary of access control configuration tasks, and an overview of the user interface.

Figure 1-2  Cisco PAM Context Diagram
Cisco PAM Server Administration Utility

The Cisco PAM Server Administration utility (Figure 1-3) is a web-based tool used to configure and monitor the Cisco PAM appliance server software. Use this utility to set up a new server, install the desktop client software, back up data, install licenses, and perform a variety of other server maintenance and monitoring tasks.

See Chapter 2, “Configuring and Monitoring the Cisco PAM Server” for more information.

*Figure 1-3  Cisco PAM Server Administration Utility*
Cisco Physical Access Gateway Administration Utility

The Cisco Physical Access Gateway Administration utility (Figure 1-4) uses a direct PC connection to enter the initial network settings on a Gateway module. You can also use the utility to upgrade firmware, and other monitoring and maintenance tasks.

See the Cisco Physical Access Gateway User Guide for instructions to use this tool.

Figure 1-4  Cisco Physical Access Gateway Administration Utility
The Enterprise Data Integration (EDI) Desktop Studio

The EDI Studio (Figure 1-5) is a desktop application used to create data integration projects for automatically synchronizing Cisco PAM with other databases, such as an HR personnel database. The EDI Studio defines the database connection, schema, and synchronization schedule used by the EDI module in Cisco PAM.

See Chapter 12, “System Integration” for more information.

Figure 1-5  EDI Studio Desktop Software

---

**Note**

This feature requires an optional Cisco license. The **EDI** menu appears only after the license is installed on the Cisco PAM server. See **Obtaining and Installing Optional Feature Licenses**, page 2-21 for more information.
Cisco Video Surveillance Viewer

The Cisco VSM Video Player is a desktop application used to archived video from the Cisco Video Surveillance Manager. See Chapter 13, “Video Monitoring” for more information.

Badge Designer

The Badge Format Editor (Figure 1-6) is included with the optional Badge Designer module to create and modify badge designs. See Chapter 8, “Configuring Personnel and Badges” for more information.

![Badge Format Editor](image)

Note

This feature requires an optional Cisco license. The Badge Designer menu appears only after the license is installed on the Cisco PAM server. See Obtaining and Installing Optional Feature Licenses, page 2-21 for more information.
CHAPTER 2

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, page 2-2
- Using Redundant Appliances for High Availability, page 2-2
- Understanding IP Addresses on the Cisco PAM Server, page 2-3
- Entering the Initial Server Configuration, page 2-4
- Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12
- Understanding the Cisco PAM Server Username and Password, page 2-16
- Obtaining and Installing Optional Feature Licenses, page 2-21
- Troubleshooting and Monitoring, page 2-26
- Next Steps, page 2-27
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 2-4.
- After the initial server configuration is complete, see Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12.

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. Whenever you upgrade the server software, you must also upgrade the desktop software. If the versions are not the same, an error occurs when launching the desktop client. See Installing or Updating the Cisco PAM Desktop Software, page 3-2.

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 2-4.
- 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.

The high availability (HA) feature requires a separate license. See Obtaining and Installing Optional Feature Licenses, page 2-21.
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 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 2-4
- Connecting a PC to the Appliance, page 2-4
- Initial Setup Instructions, page 2-5

Before You Begin

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

- A PC and web browser Internet Explorer 6.0 or 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 2-3.
- (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 cpamadmin.

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 Cisco Physical Security Multi Services Platform User Guide or Cisco Physical Access 1125 Appliance User Guide 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

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 2-2:

default username: cpamadmin
default password: cpamadmin

Figure 2-1 Cisco PAM Server Administration Utility: Login

Tip The default cpamadmin 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 process, as described in Initial Setup Instructions, page 2-5. The cpamadmin username cannot be changed.

Note See Understanding the Cisco PAM Server Username and Password, page 2-16 for more information.

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 2-4.

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

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 server in a redundant configuration. A standby server must have the exact same configuration settings as the active except the network addresses, host name, and HA license.

**Figure 2-2  Initial Setup: Server Configuration**

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 2-3. Enter the same settings on the active and standby appliance.

Figure 2-3    Initial Setup: User Configuration

![Image of Initial Setup: User Configuration]

- **Username**: The admin username cannot be changed. The default username is `cpamadmin`.
- **Current Password**: Enter the administrator password. The default password is `cpamadmin`.
- **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.
- **Re-enter Password**: Re-enter the administrator password to confirm the setting.
- **Email Address**: (Optional) Enter the email address that will receive system messages. This email address also receives Forgot Password emails (see Resetting a Forgotten Password, page 2-18).
- Select Next to apply the settings and continue.
Step 4  Enter the Network configuration for the Cisco PAM appliance, as shown in Figure 2-4.

- 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 2-4  Initial Setup: Network Configuration**

Complete the following Network settings:

- **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.

- **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 2-3 for more information.

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

- **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 2-3** 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.

    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 use of an optional Network Time Protocol server, used to automatically adjust the date and time for the Cisco PAM appliance. You can also use NTP to sync the appliance and Gateway module clocks for events and messaging.

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 2-10.
- **Option 2**: Obtain the License File from the Cisco Web Site, page 2-11.

**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 2-22 for more information. See also **Licensing: Frequently Asked Questions**, page C-1.

**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 2-22.

b. Enter the code in the PAK field, as shown in Figure 2-5.

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

**Figure 2-5**

*Initial Setup: License Installation*

![License Installation Screen](image)

**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 2-22.

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 2-5), 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 2-6. 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 2-6   Initial Setup: Setup 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 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 a menu from the tabs along the top of the window, as shown in Figure 2-7. Each tab includes additional selections on the left, or additional drop-down menus.

**Step 3** Select an option or command as described in Table 2-1 “Menus and Options in the Cisco PAM Server Administration Utility”.

**Step 4** For settings in the Setup menus, click Update to activate the changes.

*Figure 2-7  Cisco PAM Server Administration Utility: Setup Menus*
Table 2-1 describes the configuration, administration, and monitoring tasks available in the Cisco PAM Server Administration utility.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Displays information about the current and past state of the server, and includes the following submenus:</td>
</tr>
<tr>
<td></td>
<td>• Status: Displays real-time information about the current state of the Cisco PAM appliance and high availability. Includes the server software version and serial number. Also includes options to stop or start services, including the following:</td>
</tr>
<tr>
<td></td>
<td>– Web Service API: See the Cisco Physical Access Control API Reference Guide.</td>
</tr>
<tr>
<td></td>
<td>• Server Log: Displays real-time information regarding server tasks.</td>
</tr>
<tr>
<td></td>
<td>• Setup Log: Displays real-time information regarding server setup tasks performed on the appliance.</td>
</tr>
<tr>
<td></td>
<td>• Web Application Log: Displays real-time information regarding events related to server administration tasks.</td>
</tr>
<tr>
<td></td>
<td>• Audit Log: Displays a history of tasks performed by the administrator username.</td>
</tr>
<tr>
<td></td>
<td>• Console Log: Displays a real-time console log.</td>
</tr>
<tr>
<td></td>
<td>• High Availability Audit Log: Displays real-time events related to a redundant server configuration.</td>
</tr>
<tr>
<td></td>
<td>• URL Log: Displays the output (HTTP response) from URL actions.</td>
</tr>
</tbody>
</table>
Table 2-1  Menus and Options in the Cisco PAM Server Administration Utility (continued)

<table>
<thead>
<tr>
<th>Setup</th>
<th>Allows you to view and edit the server configuration using the following submenus:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Click <strong>Update</strong> to save and activate your changes.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The username, password and email of the administrator login.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>The IP address configuration for the appliance and for the Eth0 and Eth1 network ports. See Entering the Initial Server Configuration, page 2-4 for more information.</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>The DNS settings for the appliance, if DNS is used.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>The email settings for the appliance, including SMTP <strong>Server Address</strong> and SMTP <strong>Email Address from</strong>. These settings are used to send notifications and other information from the server.</td>
</tr>
<tr>
<td></td>
<td>– Click <strong>Test</strong> to send a test message and verify the settings. The test message is sent to the administrator email address entered in User settings.</td>
</tr>
<tr>
<td></td>
<td>– Select <strong>Update</strong> to apply the settings.</td>
</tr>
<tr>
<td><strong>Date &amp; Time</strong></td>
<td>The server date and time settings. If a network time protocol server is used, click NTP <strong>enable</strong> and enter the NTP <strong>Server Address</strong> settings.</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Displays the Cisco licenses installed on the appliance and allows you to install additional licenses.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Install</strong>: Install additional Cisco Physical Access Control feature licenses. See Obtaining and Installing Optional Feature Licenses, page 2-21.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Features</strong>: Displays the licensed modules currently installed in the appliance.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Files</strong>: Lists the license files installed on the appliance.</td>
</tr>
<tr>
<td><strong>Log Level</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Backup</strong></td>
<td>Creates a compressed backup file of all system and configuration data that can be used to restore a server. See Backing up the Cisco PAM Database, page A-2.</td>
</tr>
<tr>
<td><strong>Archive</strong></td>
<td>Removes historical events from the database and saves them in a password protected .zip file containing a SQL script. The file can be run on an offline database to view the purged events. Any events older than the selected Archive Date &amp; Time are included in the archive. See Archiving Historical Events, page 10-47 and Archiving the Historical Events Database, page A-4.</td>
</tr>
<tr>
<td><strong>Restore</strong></td>
<td>Restores data from a backup or archive file. The server must be stopped using <strong>Stop Server</strong> in the Commands menu. See Restoring a Server Backup File, page A-6.</td>
</tr>
<tr>
<td><strong>Upgrade</strong></td>
<td>Upgrades the server software. To upgrade the server, select <strong>Stop Server</strong> from the Commands menu, click <strong>Browse</strong> to select an upgrade file, and then click <strong>Upgrade</strong>. Select <strong>Start Server</strong> from the Commands menu when the upgrade is complete. See Upgrading the Cisco PAM Server Software, page B-7.</td>
</tr>
</tbody>
</table>
Performing Additional Configuration, Administration, and Monitoring Tasks

Table 2-1  Menus and Options in the Cisco PAM Server Administration Utility (continued)

<table>
<thead>
<tr>
<th>Commands</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Start Server: Enables the Cisco PAM access control server functions and user logins.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>When the server restarts, a message appears asking if you want to change the database password. Click Cancel or OK. This password is a security measure used for troubleshooting and technical support. It does not impact user operation,</td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>All EDI projects run when the Cisco PAM appliance is stopped and restarted. If you do not want the projects to run after a server restart, stop the project(s) before restarting the server. See Importing, Starting, and Monitoring EDI Projects in Cisco PAM, page 12-33.</td>
</tr>
<tr>
<td>• Reboot: Performs a hard reboot of the appliance which restarts the OS and the access control server.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• Show Technical Support: Collects detailed information and logs for use by Cisco technical support. This command is processor intensive and can result in decreased system performance. Use the command only under the supervision of a Cisco support representative.</td>
<td></td>
</tr>
<tr>
<td>• Processes: Displays the processes running on the system for use in troubleshooting.</td>
<td></td>
</tr>
<tr>
<td>Launch Client</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 2-2) and in the Downloads menu.
### Understanding the Cisco PAM Server Username and Password

The `cpamadmin` username is the only username for the Cisco PAM Server Administration utility. The `cpamadmin` username cannot be changed and additional usernames cannot be added. The default password (also `cpamadmin`) must be changed during the initial server setup.

*Note:

The same `cpamadmin` username and password is automatically created on the Cisco PAM desktop client during the initial server setup. After the initial server setup, however, the desktop `cpamadmin` username and password is managed separately: changes to the server password do not affect the desktop account. See Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client” for more information.

This section includes instructions to change the server password, or to recover a forgotten password. To recover a forgotten password: click the **Lost Password?** link on the login page. The **Lost Password?** link is available only if the server email settings are configured since the link is used to send an email with a reset instructions.

If the **Lost Password?** link is not enabled, you must recover the password by reinstalling the server software.

This section includes the following information:

- Changing the Cisco PAM Server Administration Utility Password, page 2-17
- Resetting a Forgotten Password, page 2-18
- Recovering a Lost Server Password, page 2-20
Changing the Cisco PAM Server Administration Utility Password

To change the password for the *cpamadmin* username on 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 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.

**Step 2** Select the Setup tab and then select the User menu, as shown in Figure 2-8.

**Figure 2-8  Cisco PAM Server Administration Utility: Setup Menus**

![Cisco PAM Server Administration Utility: Setup Menus](image)

**Step 3** Enter the current and new passwords in the appropriate fields.

**Step 4** Click Update.

**Note** Changing the server password does not effect the *cpamadmin* user password for the Cisco PAM desktop client. See Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client” for information on managing desktop client usernames and passwords.
Resetting a Forgotten Password

To reset a forgotten `cpamadmin` server password, click the **Forgot Password?** link on the login page and complete the following instructions.

---

**Note**
- The **Forgot Password?** link appears only if the feature is enabled (as described in Enabling the **Forgot Password Feature**, page 2-19). If the **Forgot Password?** link does not appear on the login page, follow the instructions in the “Recovering a Lost Server Password” section on page 2-20.
- The server password is different from the Cisco PAM desktop client password. See Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client” for information on managing desktop client usernames and passwords.

---

To reset a forgotten admin password for the server utility, do the following:

**Step 1**  
Open the Cisco PAM Server Administration utility login page.

**Step 2**  
Click the **Forgot Password?** link, as shown in Figure 2-9.

---

![Figure 2-9  
Forgot Password Link](image)

When you click this link, an email containing password instructions is sent to the email address configured in the **User** setup page.

**Step 3**  
Access the email in your email application, and click the included URL to open an online reset password form, as shown in Figure 2-10.

---

**Note**  
The email URL is only valid for 30 minutes, or until used to reset the password.
Enabling the Forgot Password Feature

The Forgot Password? link appears on the login page only if the server email settings are configured, as described in the following steps.

Step 1 Log in to the Cisco PAM Server Administration utility.
Step 2 Enter the email address that will receive Forgot Password? emails.
   a. Select the Setup tab and then select the User menu, as shown in Figure 2-11.
   b. Enter an Email Address that will receive Forgot Password emails.
c. Click **Update**.

**Step 3**
Enter the SMTP settings used to send the Forgot Password emails.

a. In the **Setup** tab, click the **Email** menu, as shown in **Figure 2-12**.

**Figure 2-12 Send Email Settings for Forgot Password**

![Image of Cisco PAM Server Administration with Send Email Settings panel]

b. Enter the **SMTP Server Address** used to send outgoing messages. Outgoing messages also include event and other alarm information.

c. Enter an email address in **SMTP Email Address from**. This address appears in the **From** field for messages sent by the Cisco PAM appliance. This email address is also the **Reply To** address.

d. Click **Test** to verify the settings.

e. Click **Update** to save the settings.

---

**Recovering a Lost Server Password**

If the **cpamadmin** password is lost and the **Forgot Password?** feature is not enabled, do the following.

**Step 1**
Reinstall the server software and enter a new **cpamadmin** password, as described in Reinstalling the Cisco PAM Server Software from a Recovery CD, page B-14. Reinstalling the Cisco PAM server software deletes all server information and settings.

**Step 2**
Restore the Cisco PAM data and settings from a backup file, as described in Appendix A, “Backing Up and Restoring Data”.

**Note**
The backup file does not include the old password. The password is entered during the restore.
Obtaining and Installing Optional Feature Licenses

The Cisco PAM appliance includes a base package of software licenses to enable access control:

- Release 1.0.0 includes a 4 module base license
- Release 1.1.0 and later includes a 32 modules base license.

To enable additional licensed features, such as support for additional hardware modules or the Badge Designer, complete the instructions in this section.

Note

- 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 2-4 to install licenses during the initial setup.
- 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 2-21
- Licenses in a Redundant Configuration, page 2-22
- Purchasing Additional Feature Licenses, page 2-22
- Installing Additional Licenses, page 2-23
  - Option 1: Enter the Product Authorization Key to Download the License File, page 2-23.
  - Option 2: Obtain the License File from the Cisco Web Site, page 2-24.
- Displaying the Cisco PAM Appliance Serial Number, page 2-25
- Displaying a Summary of Installed Licenses, page 2-25

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 2-22 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.

Note

For answers to common licensing questions, see Licensing: Frequently Asked Questions, page C-1.
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 2-4.

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 2-2: 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 2-25 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 2-23 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 2-2 lists the part numbers for the optional feature licenses.

<table>
<thead>
<tr>
<th>Part</th>
<th>Optional Feature Licence</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIAC-PAME-M64=</td>
<td>Cisco Physical Access Manager 64-module capacity upgrade license</td>
</tr>
<tr>
<td>CIAC-PAME-M128=</td>
<td>Cisco Physical Access Manager 128-module capacity upgrade license</td>
</tr>
<tr>
<td>CIAC-PAME-M512=</td>
<td>Cisco Physical Access Manager 512-module capacity upgrade license</td>
</tr>
<tr>
<td>CIAC-PAME-M1024=</td>
<td>Cisco Physical Access Manager 1024-module capacity upgrade license</td>
</tr>
<tr>
<td>CIAC-PAME-BD=</td>
<td>Cisco Physical Access Manager Badge Designer and Enroller</td>
</tr>
<tr>
<td>CIAC-PAME-HA=</td>
<td>Cisco Physical Access Manager High-Availability License</td>
</tr>
<tr>
<td>CIAC-PAME-EDI=</td>
<td>Cisco Physical Access Manager Enterprise Data License</td>
</tr>
<tr>
<td>CIAC-PAME-WSAPI</td>
<td>= Cisco Physical Access Manager Web Services API</td>
</tr>
</tbody>
</table>
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.

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 2-4.

This section includes the following information:

- Option 1: Enter the Product Authorization Key to Download the License File, page 2-23
- Option 2: Obtain the License File from the Cisco Web Site, page 2-24

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 2-2.

**Step 3** Enter the PAK code, as shown in Figure 2-13.

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

![Figure 2-13 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 2-24.
Step 5  Select the **Features** tab to verify that the new license was added. See Displaying a Summary of Installed Licenses, page 2-25 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 2-13 on page 2-23), 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 2-25 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 2-14.

Figure 2-14  License Features List

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 2-15.

Step 3  Refer to the entry for Serial Number.
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**, **Reboot**, or **Shut Down**. See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12 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.

Troubleshooting and Monitoring

See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12 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.

For information on feature licenses, see Licensing: Frequently Asked Questions, page C-1.
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 3, “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.
CHAPTER 3

Getting Started With the Cisco PAM Desktop Software

This chapter describes how to install the Cisco PAM desktop client software, log on to Cisco PAM, and begin configuring access control features and doors. This chapter also includes an overview of the Cisco PAM user interface.

Tip

See Installation and Configuration Summary, page 1-3 for an overview of installation and configuration tasks.

Contents

- Before You Begin, page 3-2
- Installing or Updating the Cisco PAM Desktop Software, page 3-2
- Logging in to Cisco PAM, page 3-3
- Understanding the Start Page and Window Management, page 3-4
- Keeping a Module On Top, page 3-6
- User Interface Elements, page 3-8
- Toolbar Features, page 3-10
  - Creating Reports, page 3-10
  - Using Filters, page 3-12
  - Revising the Column Display, page 3-14
  - Using Group Edit, page 3-14
  - Search, page 3-15
Before You Begin

Before you begin using the Cisco PAM desktop software to configure Cisco Physical Access Control, do the following:

- Verify that your computer is connected to the Internet, including access to the Cisco PAM appliance Cisco Physical Access Control IP network.
- Verify that your PC meets the following requirements:
  - Microsoft Windows XP or Vista
  - Java 6.0 or higher (JDK 1.6 or higher). To download Java, go to http://www.java.com/en/download/manual.jsp.
  - 2.8 GHz Intel Pentium IV processor or higher.
  - 1GB RAM or more.
  - 100 MB hard disk space available for the application, and an additional 20 GB or more disk space for data storage.
- Obtain your username and password from your system administrator.

Installing or Updating the Cisco PAM Desktop Software

To install the desktop software, you must connect to the Cisco PAM Server Administration utility. Always upgrade the Cisco PAM desktop client when the server software is upgraded. If the versions are not the same, an error occurs when launching the desktop client.

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

- To use a direct connection, see Connecting a PC to the Appliance, page 2-4.
- To use an Internet connection, open a web browser and enter the IP address used for the Cisco PAM Server Administration utility. See Understanding IP Addresses on the Cisco PAM Server, page 2-3, or ask your system administrator for assistance.

**Step 2** Select **Launch Cisco PAM Client** from the Login window, as shown in Figure 3-1.

- If the correct version of the Cisco PAM desktop is already installed on your PC, the application launches.
- If the client is not installed, or is out of date, the software is installed or updated on your PC. The Java runtime environment software is also installed or updated.
- If the download fails, check your Java Web Start network settings. The Cisco PAM client launches using Java Web Start.
Logging in to Cisco PAM

Launch the Cisco PAM desktop client software to display the login prompt (Figure 3-2).

**Step 1** Enter the server IP address of the Cisco PAM appliance. Click the arrow next to the field to select a previous entry (the system remembers the last five server addresses).

**Step 2** Enter your username and password (both are case-sensitive) and click **Log In**.

**Note** Ask your system administrator for the correct username and password.

For additional methods to install or upgrade the Cisco PAM desktop software using the Cisco PAM Server Administration utility, see Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12.
If the username and password are valid, Cisco Physical Access Manager displays the **Start Page**, or the modules that were open during the operator's previous session.

**Tip**

To change your password, log on to the Cisco PAM appliance and select **Change Password** from the **Options** menu.

### Understanding the Start Page and Window Management

The Start Page is opened by default when you open the Cisco PAM desktop client for the first time, as shown in **Figure 3-3**. The main menus provide access to Cisco PAM features, and are also displayed in the main window for each feature.

**Figure 3-3  Cisco PAM Start Page**

The available modules vary depending on the software license purchased and the operator's access privileges. Some menus are activated only after the feature license is installed. See **Obtaining and Installing Optional Feature Licenses**, page 2-21 and Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client”.
Select a menu item to open the main window for that feature in a new window, as shown in Figure 3-4. You can open multiple module windows simultaneously and drag the windows across multiple monitors. The size and position of the open windows is restored when you log out and log back in.

**Figure 3-4  Device Templates Main Window**
Keeping a Module On Top

You can configure a Cisco PAM module to be always displayed on top. When Cisco PAM is open, the selected module always remains on top of other Cisco PAM windows, or any other applications.

To configure a window to always be on top:

**Step 1** Select **Always on Top** from the Options menu, as shown in Figure 3-5.

**Step 2** Click OK to close the confirmation message.

**Step 3** Close the window and reopen it for changes to take effect.

**Tip**

Before closing the window, be sure another Cisco PAM module is open or the application will quit.

**Figure 3-5 Always on Top**

When selected, **Always on Top** is displayed with a check (Figure 3-7). The setting remains in effect even if you close and then reopen the window.
Choosing Multiple *Always on Top* Windows

You can select more than one window to be on top. The windows remain on top of all other windows, except each other. Click an *Always on Top* window to bring it to the front.

When you select additional *Always on Top* windows, you must click the confirmation message (Figure 3-6), and then close and reopen the window.

**Note**

If the confirmation message is hidden behind an existing Window on Top, rearrange the windows so you can clear the message.

---

**Figure 3-6 Always on Top Confirmation Message**

![Confirmation Message Image]

---

Deselecting *Always on Top*

To deselect *Always on Top*, do the following:

**Step 1**  
Deselect *Always on Top* to remove the check (Figure 3-7).

**Step 2**  
Click **OK** to close the confirmation message (Figure 3-6). If the confirmation message is hidden behind an existing Window on Top, rearrange the windows so you can clear the message.

**Step 3**  
Close the Cisco PAM window and reopen it for changes to take effect.

**Step 4**  
Repeat these steps to deactivate *Always on Top* for additional windows.

---

**Figure 3-7 Deselecting Always on Top**

![Deselecting Always on Top Image]
User Interface Elements

The user interface for most features includes the following elements:

**Figure 3-8** User Interface Elements

The following items are shown in Figure 3-8:

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Window Title Bar</td>
<td>Shows the module and application name (for example: Events - Cisco Physical Access Manager).</td>
</tr>
<tr>
<td>2 Menu Bar</td>
<td>Allows the operator to perform a number of functions, including open a new module, close a module or the application, and get help. The menu bar is the same for all modules.</td>
</tr>
<tr>
<td>3 Table Columns</td>
<td>Column visibility and order may be edited using the Columns... button. Column width may be adjusted by dragging the edge of the column header. Clicking the column header allows the list to be sorted by a particular column. A directional arrow shows the current sort column, as well as the direction. Clicking the column header a second time reverses the sort order. See Revising the Column Display, page 3-14.</td>
</tr>
</tbody>
</table>
## Table 3-1  User Interface Elements

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4</strong> Toolbar</td>
<td>Contains a set of button functions that are specific to the module being used. Typical buttons include:&lt;br&gt;  - <strong>Scroll Lock</strong>: Disable or enable automatic scrolling of the list as new items are inserted.&lt;br&gt;  - <strong>View... or Edit...</strong>: View or edit the selected item in a detail window.&lt;br&gt;  - <strong>Add...</strong>: Add a new item.&lt;br&gt;  - <strong>Disable or Delete</strong>: Disable or delete the selected item.&lt;br&gt;  - <strong>Report...</strong>: Display the available data as a report, which may be printed or saved as a PDF. See Creating Reports, page 3-10.&lt;br&gt;  - <strong>Filter</strong>: Select or edit a filter. This determines which items are visible in the table. See Using Filters, page 3-12.&lt;br&gt;  - <strong>Columns...</strong>: Configure which columns are visible, and the order in which they appear. See Revising the Column Display, page 3-14.&lt;br&gt;  - <strong>Group Edit</strong>: Make changes to all items displayed in a module table. See Using Group Edit, page 3-14.&lt;br&gt;  - <strong>Quick Search</strong>: Quickly search results in the main module window. See Search, page 3-15.</td>
</tr>
<tr>
<td><strong>5</strong> Table</td>
<td>Shows a list of items. Selecting an item within the table enables the use of certain buttons, and right-clicking an item brings up a menu of actions performable upon that item. Each module will have a different table.</td>
</tr>
<tr>
<td><strong>6</strong> Status Bar</td>
<td>Appears at the bottom of each module window. It is divided into 4 panes:&lt;br&gt;  - <strong>Pane 1</strong>: If there are any uncleared alarms, this pane displays a colored and or blinking icon showing the alarm status. This pane is not pictured in the above figure.&lt;br&gt;  - <strong>Pane 2</strong>: If there are any uncleared alarms, this pane displays text describing the number of alarms, as well as their state. This pane is not pictured in the above figure.&lt;br&gt;  - <strong>Pane 3</strong>: Shows the number of items in the table.&lt;br&gt;  - <strong>Pane 4</strong>: Displays the username of the logged-in operator, as well as the IP address or hostname they are logged in from.</td>
</tr>
</tbody>
</table>
Toolbar Features

The toolbar includes a common set of features used to sort and revise information and records. This section includes the following information:

- Creating Reports, page 3-10
- Using Filters, page 3-12
- Revising the Column Display, page 3-14
- Using Group Edit, page 3-14
- Search, page 3-15

Creating Reports

Many Cisco PAM modules include a Report feature. The following example describes how to create an Events report.

Step 1  Open the desired module (in this case the Events module) by selecting it from the Start Page or from the Module menu.

Step 2  Click the Report... button in the toolbar. This opens the Report Generation window (Figure 3-9).

Figure 3-9  Report Generation Window

The following items are shown in Figure 3-9:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The title of the report.</td>
</tr>
<tr>
<td>Include available</td>
<td>Depending on the type of objects in the report (event, badge, personnel</td>
</tr>
<tr>
<td>details in report</td>
<td>record, etc.), there may be additional details that are available to be</td>
</tr>
<tr>
<td></td>
<td>included in the report. If so, these will be available as checkboxes. For</td>
</tr>
<tr>
<td></td>
<td>example, in a report of personnel records, checking the Badges option will</td>
</tr>
<tr>
<td></td>
<td>include a list of badges assigned to each person.</td>
</tr>
<tr>
<td>Group by</td>
<td>If this option is set to something other than [None], the items in the</td>
</tr>
<tr>
<td></td>
<td>report will be grouped by the specified property, with a header for each</td>
</tr>
<tr>
<td></td>
<td>group.</td>
</tr>
</tbody>
</table>
Chapter 3      Getting Started With the Cisco PAM Desktop Software

Step 3
Choose the desired options, and then click OK to save or open the report. This may take a moment, depending on the size and complexity of the report. Figure 3-10 shows a report in PDF format from the Events module.

Figure 3-10    Events Report in Report Viewer

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
<th>Device</th>
<th>Address</th>
<th>Personnel</th>
<th>Record</th>
<th>Date</th>
<th>Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/1/2010 03:18:59</td>
<td>Logical Driver Started</td>
<td>Logical Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/1/2010 03:18:59</td>
<td>Logical Driver Started</td>
<td>Logical Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/1/2010 03:18:59</td>
<td>EID Driver Started</td>
<td>EID Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/1/2010 03:18:59</td>
<td>Logical Driver Started</td>
<td>Logical Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/1/2010 03:18:59</td>
<td>EID Driver Started</td>
<td>EID Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/1/2010 03:18:59</td>
<td>Gateway Driver Started</td>
<td>Gateway Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9/1/2010 03:18:59</td>
<td>Access EID Driver</td>
<td>Access EID Driver</td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using Filters

Many Cisco PAM modules include a **Filter** button that provide the following options:

- **No Filter**: Show all items, without filtering.
- **Default Filter**: The default view of the table. Shows all enabled items.
- **Presets**: Select from preset filters. A check mark next to the filters displays which filter is currently in use, as shown in Figure 3-12.
- **Preset Manager...**: Manage the presets.
- **Edit Filter...**: View or edit the current filter.
- **Max rows...**: Specify the maximum number of items (rows) to be displayed. Some items, such as events, often exist in such large quantities that viewing them all simultaneously is impractical.

When editing or viewing a filter, the operator may select or enter the various criteria to filter by. In addition, the following actions are available:

- **View Query...**: View the filter as an SQL-like expression. This feature is intended for advanced operators.
- **Save as Preset...**: Save the current filter as a preset, which can be quickly accessed from the **Filter** button.
- **Reset**: Reset the filter to the default.
- **OK**: Apply the changes to the filter and close.
- **Cancel**: Cancel any changes to the filter and close.

**Filter Example**

To create a filter in the **Events** module, do the following:

**Step 1** Select **Events** from the Events & Alarms menu, in the Monitoring sub-menu.

**Step 2** Click **Filter** in the toolbar to open the filter window, as shown in Figure 3-11.
Step 3 Specify the object filtering criteria:

- The **General, Personnel Record, Credential, Badge, Login, and Device** tabs on the left specify the event criteria, such as the event's properties or associated objects.
- The **View Query...** button opens a window detailing the actual filter definition as an SQL-like expression string.
- The **Save as Preset...** button saves the filter criteria as a named preset for later use. Once a filter is saved as a preset, it can be selected from the **Filter** button drop-down menu, as shown in **Figure 3-12**.
- The **Reset** button clears the filter so that all enabled items will be displayed.
Step 4  Choose the criteria to filter by, then click the OK button. This closes the window, and the table view is updated to reflect the filter criteria. Incoming events will also be filtered according to these criteria.

Revising the Column Display

The Columns... button in the toolbar allows you to change the order and visibility of columns. Click the Columns... button to open the window shown in Figure 3-13.

- Select or deselect the checkboxes next to the column names to determine which columns are visible in the table view.
- Select a column name and click the Up and Down buttons to change the order that the columns appear.
- Click OK to save your changes and view them in the module.

![Figure 3-13  Columns Window for the Event Manager]

Tip  Adjust column width by dragging the edge of the column header. Click on a column header to sort the table by that particular column. A directional arrow shows the currently sorted column, as well as its direction. Reverse the sort order by clicking on the column header a second time.

Using Group Edit

The Group Edit button allows you to make changes to all items in a list, or multiple selected items. Group Edit... is included in the Badges and Personnel modules.

Tip  To limit the items in the list, filter the content as described in Using Filters, page 3-12 before using group edit.

Right-click the Group Edit button in the Badges and Personnel and select Group Edit All Items or Group Edit Selected Items.
Group Edit Example

In the following example, a group edit is used to change all contractor issued badges to inactive.

Step 1  Select Badges from the User menu.

Step 2  Filter the list so it contains only the records to be changed.
   a. Click the Filter button in the toolbar.
   b. Select the Assigned to tab.
   c. Select Contractor in the Personnel type field.
   d. Click OK to filter the badges to contractor personnel types.

See Using Filters, page 3-12 for more information.

Step 3  In the Badges window, click the Group Edit... button to open the Group Edit... window, as shown in Figure 3-14.

Figure 3-14  Group Edit - General Window

Step 4  Select the Validity checkbox, and then select Inactive from the drop-down menu.

Step 5  Click OK.

Step 6  All Contractor badges in the filtered list are now changed to Inactive.

Search

Search allows operators to quickly search results in the main module window. Type in a search field and click the Search button or press the Enter key. To remove the search clear it out and click the Search button.

Use the drop down arrow to select the different methods of quick search. Options include:

- **Quick search with filter**: Search within the results of the current Filter set.
- **Quick search instead of filter**: Search without regard to any filter that is currently defined.
CHAPTER 4

Configuring User Access for the Cisco PAM Desktop Client

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

Note
Whenever you upgrade the server software, you must also upgrade the desktop software. If the versions are not the same, an error will occur when launching the desktop client. See Installing or Updating the Cisco PAM Desktop Software, page 3-2.

Contents

- Defining User Profiles for Desktop Application Access, page 4-2
- Creating User Login Accounts and Assigning Profiles, page 4-8
- Configuring LDAP User Authentication, page 4-11
- Viewing Audit Records for Changes to Usernames, page 4-15
- Managing Desktop Client Passwords, page 4-16
Defining User Profiles for Desktop Application Access

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

**Note**
The Administrators profile is read-only and cannot be changed.

To create profiles, do the following:

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

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

**Figure 4-1 Profiles Module Main Window**

![Profiles Module Main Window](image)

**Tip**
To modify an existing profile, select the entry and choose Edit. To remove a profile, select the entry and choose Delete. The Administrators profile is read-only and cannot be changed.

**Step 3** Select a Profile template that most closely matches the desired level of user access, as shown in Figure 4-2:
- **Default**: a basic set of privileges is set
- **Most Restrictive**: no privileges are set.
- **Least Restrictive**: all privileges are set.

**Figure 4-2 Profile Templates**

![Profile Templates](image)
Step 4  Enter the basic profile settings, as shown in Figure 4-3.

**Figure 4-3  Profile: General Tab**

![Profile: General Tab](image)

a. **Profile name**: Enter a descriptive name for the profile.

b. **Enabled**: Select the check box to enable the profile, or deselect the box to disable the profile.

c. **Partition**: Select the partition from the drop-down menu.

Step 5  Click the **General** tab to define the basic profile properties. Click the check box next to each field to enable or disable the privilege, as described in Table 4-1.

**Table 4-1  General Settings: Profile Module**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Allow access to the application</td>
<td>Allows access to the application.</td>
</tr>
<tr>
<td>Allow issuing device commands</td>
<td>Allows user to issue device commands directly to hardware.</td>
</tr>
<tr>
<td>Allow access to external hyperlinks</td>
<td>Allows access to external hyperlinks.</td>
</tr>
<tr>
<td>Require device commands to be commented</td>
<td>Requires the user to enter a comment with each device command issued in the system.</td>
</tr>
<tr>
<td>Allow editing from right-click menus</td>
<td>Allows access to the right-click Edit menu.</td>
</tr>
<tr>
<td>Allow logoff without password</td>
<td>Allows user to logoff without a password.</td>
</tr>
<tr>
<td><strong>Events/Alarms: Alarm Annotations (Ack., Clear, Comment)</strong></td>
<td></td>
</tr>
<tr>
<td>Allow annotations</td>
<td>Allows user to acknowledge, clear, and comment alarms. Click the Filter button to define the events that trigger the action.</td>
</tr>
<tr>
<td>Allow multiple annotations</td>
<td>Allows the user to acknowledge, clear, and comment multiple alarms at one time.</td>
</tr>
<tr>
<td>Allow clearing of unacknowledged alarms</td>
<td>Allows the user to clear unacknowledged alarms from active devices.</td>
</tr>
<tr>
<td>Allow clearing of active device alarms</td>
<td>Allows the user to clear alarms from active devices.</td>
</tr>
</tbody>
</table>
### Table 4-1  General Settings: Profile Module (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Events/Alarms: On new alarms</strong></td>
<td></td>
</tr>
<tr>
<td>Open Alarms Module</td>
<td>The <strong>Alarms</strong> module automatically opens with new system alarms. Click the <strong>Filter</strong> button to define the events that trigger the action.</td>
</tr>
<tr>
<td>Open Manage Alarm window</td>
<td>The <strong>Alarms</strong> module automatically opens with new system alarms. Click the <strong>Filter</strong> button to define the events that trigger the action.</td>
</tr>
<tr>
<td>Open graphic map</td>
<td>The <strong>Graphic Map</strong> module automatically opens with new system alarms. Click the <strong>Filter</strong> button to define the events that trigger the action.</td>
</tr>
<tr>
<td>Show recorded video</td>
<td>Displays recorded video with new system alarms. Click the <strong>Filter</strong> button to define the events that trigger the action.</td>
</tr>
<tr>
<td>Show live video</td>
<td>Displays live video with new system alarms. Click the <strong>Filter</strong> button to define the events that trigger the action.</td>
</tr>
<tr>
<td><strong>Help:</strong></td>
<td>defines access to the different help systems.</td>
</tr>
<tr>
<td>Allow access to help documentation</td>
<td>Allows access to help documentation.</td>
</tr>
<tr>
<td>Enable context menu in help browser</td>
<td>Allows the user to view the help context menu.</td>
</tr>
<tr>
<td>Allow access to help PDF</td>
<td>Allows the user to access the help PDF.</td>
</tr>
<tr>
<td>Note</td>
<td>Adobe PDF viewer is required.</td>
</tr>
</tbody>
</table>
Step 6  Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 4-4.

a. Select a Cisco PAM module.

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

![Profile: Modules Tab](image)

Figure 4-4  **Profile: Modules Tab**

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

Example

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

- 1. Create a profile with access to the Events module, as described in the previous steps.
- 2. Click **Default Filter**, as shown in Figure 4-4.
- 3. Select the **Device** tab, as shown in Figure 4-5.
- 4. Click **Choose**.
- In the Choose Devices window, expand the Logical Driver device tree and select a door (Figure 4-5).
- 5. Click **OK** to save the changes and close the windows.
Step 7  Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 4-6).

**Figure 4-6  Profile: Device Commands Tab**

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

b. Highlight a command.
c. Select the following options:

- **Allow Command to be issued:**
  - **Default:** If user has access to issue device commands, the command access is enabled by default.
  - **No:** Deny access to the command.
  - **Yes:** Allow access to the command.

- **Filter:** Apply a filter to limit the devices for the command.

**Step 8** Click the **Data Types** tab to define the data available to the profile, as shown in **Figure 4-7**.

**Figure 4-7**  *Profile: Data Types Tab*

![Profile: Data Types Tab](Image)

- a. Select a module and the type of data in the list.
- b. To restrict the data, click the check boxes for the following properties:

**Table 4-2**  *Profile: Data Types*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Allows the user to view the selected data type.</td>
</tr>
<tr>
<td>Create</td>
<td>Allows the user to add and create the selected data types.</td>
</tr>
<tr>
<td>Modify</td>
<td>Allows the user to modify existing data.</td>
</tr>
<tr>
<td>Delete</td>
<td>Allows the user to delete data.</td>
</tr>
<tr>
<td>Default Filter...</td>
<td>Allows the user to apply a default filter to limit objects from view.</td>
</tr>
</tbody>
</table>
Creating User Login Accounts and Assigning Profiles

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

**Step 1** Select **Logins** from the Users menu. The main window (Figure 4-8) lists all the usernames in the system.

**Figure 4-8 Logins Module Main Window**

For each login, you can:

- **Step 2** To add a login, choose **Add**.
  - To modify an existing login, select the entry and choose **Edit**.
  - To remove a login, select the entry and choose **Delete**.

**Note** Most properties of the **cpamadmin** login are read-only.

**Step 9** Click **Save and Close** to save the profile settings.

**Step 10** Assign the profile to one or more Cisco PAM operators using the **Logins** module. See **Creating User Login Accounts and Assigning Profiles**.
Step 3  Complete fields in the General tab, as shown in Figure 4-9. Table 4-3 describes the field properties.

**Figure 4-9  Logins Module: General Tab**

![Logins Module: General Tab](image)

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

**Table 4-3  General Tab Fields.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Required. The username of the login.</td>
</tr>
<tr>
<td>Password</td>
<td>Required. Password to access the system.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Required. The value must be entered exactly as it was in the <code>Password</code> field.</td>
</tr>
<tr>
<td>Assigned to</td>
<td>The personnel record the login is assigned to.</td>
</tr>
<tr>
<td>Validity</td>
<td><code>Active</code> or <code>Inactive</code>. Only active accounts can access the system.</td>
</tr>
<tr>
<td>Effective</td>
<td>The beginning date the user can log in. If left blank, the user can log in immediately.</td>
</tr>
<tr>
<td>Expires</td>
<td>The day the login expires and access is denied. If left blank, access is allowed indefinitely.</td>
</tr>
<tr>
<td>Site</td>
<td>Read-only. A site is a single instance of a Cisco PAM database.</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments or notes about the login.</td>
</tr>
</tbody>
</table>

Step 4  Assign access privileges for the login:

a. Select the `Profiles` tab, as shown in Figure 4-10.

b. Select the checkbox next to each profile to enable or disable access rights as defined by the access profile. See Defining User Profiles for Desktop Application Access, page 4-2 for more information.
c. Click **Save and Close** to save the changes and close the window.

Tip

To create a new access profile, click the **New** button to open the Profiles module and refer to [Defining User Profiles for Desktop Application Access, page 4-2](#).

**Figure 4-10 Assign One or More Profiles**

![Assign One or More Profiles](image)

**Step 5**

To verify the changes, log off and then log in with the new username and password. Verify that you can access the modules and functions specified by the assigned profiles.
Configuring LDAP User Authentication

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

- Configure the LDAP Server, page 4-11
- Create the LDAP User Account in Cisco PAM, page 4-13

Configure the LDAP Server

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

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

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

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

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

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

For more information, see the following:

- LDAP Example: User Principal Name, page 4-12
- LDAP Example: sAMAccountName, page 4-13

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

<table>
<thead>
<tr>
<th><strong>Table 4-4</strong> LDAP System Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Enable LDAP</td>
</tr>
<tr>
<td>LDAP server URL</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Principle suffix</td>
</tr>
<tr>
<td>Principle prefix</td>
</tr>
</tbody>
</table>

Cisco Physical Access Manager User Guide
Configuring LDAP User Authentication

Step 4

Restart the Cisco PAM application to enable the changes.

LDAP Example: User Principal Name

In the example shown in Figure 4-11, the user principal name is cpsm.user@ad1.cpamlab. The Cisco PAM user login must be the same (cpsm.user).

Table 4-4 LDAP System Configuration Settings (continued)

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

LDAP Example: User Principal Name

In the example shown in Figure 4-11, the user principal name is cpsm.user@ad1.cpamlab. The Cisco PAM user login must be the same (cpsm.user).
LDAP Example: sAMAccountName

In the example shown in Figure 4-12, the user login is the same as the samaccount name (cspsmuser).

Figure 4-12 sAMAccountName: LDAP Configuration Example

Create the LDAP User Account in Cisco PAM

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

Step 1 Select Logins from the Users menu.

Figure 4-13 Login Window: LDAP Login Type
Chapter 4  Configuring User Access for the Cisco PAM Desktop Client

Configuring LDAP User Authentication

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

Step 3  Select the Login type LDAP. The Login type field appears only if LDAP was enabled and the Cisco PAM application was restarted (see Configure the LDAP Server, page 4-11).

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

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

Step 5  Click Profiles and select the user’s Cisco PAM profiles. See Defining User Profiles for Desktop Application Access, page 4-2 for more information.

Note  Cisco PAM does not synchronize the LDAP profiles.

Step 6  Click Save and Close.
Viewing Audit Records for Changes to Usernames

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

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

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

**Step 3** Select **Audit Records**, as shown in Figure 4-14.

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

*Figure 4-14  Logins Audit Records Window*

*Table 4-5  Logins Module: Audit Records Fields*

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

- Changing Your Password, page 4-16
- Changing Another User’s Password, page 4-16
- Managing the cpamadmin Login and Password, page 4-17

Tip
To determine password expiration and strength requirements, see Password Policy Settings, page 14-5.

Changing Your Password

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Options menu, select Change Password.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter your old password, and then enter a new password.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Re-enter the new password to confirm the setting.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

Changing Another User’s Password

To change another user’s password, edit the Login record for that user. See Creating User Login Accounts and Assigning Profiles, page 4-8 for instructions.

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

Table 4-5 Logins Module: Audit Records Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential</td>
<td>The username used when the modification occurred. Click View to display and</td>
</tr>
<tr>
<td>Personnel record</td>
<td>The name of the operator associated with the modification (if the login</td>
</tr>
<tr>
<td>Data</td>
<td>Additional information about the modification.</td>
</tr>
<tr>
<td>View Current...</td>
<td>Opens a new window displaying the current settings.</td>
</tr>
<tr>
<td>View Before...</td>
<td>Opens a new window displaying the settings before the change was made.</td>
</tr>
<tr>
<td>View After...</td>
<td>Opens a new window displaying the settings after the change was made.</td>
</tr>
</tbody>
</table>
Managing the `cpamadmin` Login and Password

The `cpamadmin` login and password are created during the initial server setup, as described in Chapter 2, “Configuring and Monitoring the Cisco PAM Server”. After the initial setup, however, the `cpamadmin` login and password for the desktop client are managed independently of the server login: changes to the desktop login do not effect the server login. See Understanding the Cisco PAM Server Username and Password, page 2-16 for more information.

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

![Expanded Hardware Tree: Gateways and Related Devices](image)

Some devices, such as tamper inputs, fire sensors, and cameras, are not part of door configurations.
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>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>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>
<tr>
<td>Access GW Driver</td>
<td>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.</td>
</tr>
<tr>
<td>Gateway Controller</td>
<td>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.</td>
</tr>
<tr>
<td>Access Control</td>
<td>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”.</td>
</tr>
</tbody>
</table>
Chapter 5      Understanding Door Configuration

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>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Module Interface&lt;br&gt;Each module includes a set of interfaces for connecting door hardware and other devices. For descriptions of each module interface, see the Cisco Physical Access Gateway User Guide.</td>
</tr>
<tr>
<td>7</td>
<td>Devices&lt;br&gt;Devices include hardware such as card readers and locks. Device configurations are applied using pre-defined templates, or for a specific interface. See Chapter 6, “Configuring Doors” and Chapter 7, “Configuring Door and Device Templates”.</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.

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).

Figure 5-4  Locations & Doors: View Menu

![Locations & Doors: View Menu](image)

To execute a command for all the devices or doors in a location, right-click the location and select a command.

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.
- or
- 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**

![Hardware module screenshot]

**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>![Mixed Color 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**

- **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

![Recent Events Table]

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.

*Note* If a topic does not display any information when expanded, then no criteria meets that condition.

**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.

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.

**Note** Changes made to door, device, and credential templates also change any doors or devices configured with those templates.

- **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 affect 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 use 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

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

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

**Step 4**

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><strong>Step 4</strong> Apply the door configuration changes. Right-click a location or Gateway and select <strong>Apply Configuration Changes</strong>. <strong>Note</strong> 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.</td>
<td><img src="" alt="Diagram of Cisco Physical Access Manager interface" /></td>
</tr>
</tbody>
</table>
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*. 
Configuring Doors

A door configuration is a set of device hardware, such as locks and readers, assigned to a Gateway’s interfaces. This chapter includes instructions to create and modify door configurations.

Tip
You can create the door configuration before the related Gateway is physically installed and added to the network. See Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2 for more information.

Contents

- Configuring Doors, page 6-2
  - Adding Gateways and Doors Using Templates, page 6-2
  - Adding Doors Using Door Templates, page 6-7
- Modifying Door Configurations, page 6-14
- Applying Configuration Changes, page 6-17
- Disabling or Deleting a Device or Door, page 6-19
- Cloning a Gateway Configuration, page 6-27
- Configuring Device Groups, page 6-28
- Replacing a Gateway or Expansion Module, page 6-31
- Changing Gateway Passwords, page 6-31
- Device and Driver Commands in the Hardware Device View, page 6-34
- Door Modes, page 6-39
- Door Commands, page 6-39
Configuring Doors

This section includes the following information.

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

Adding Gateways and Doors Using Templates

Use Gateway templates to quickly add a new Gateway configuration. Once the Gateway is added to the system, you can configure one or more door configurations.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Create the locations for door and devices.</td>
<td><img src="image" alt="Locations &amp; Doors" /></td>
</tr>
<tr>
<td>a. Select Locations &amp; Doors from the Doors menu.</td>
<td></td>
</tr>
<tr>
<td>b. To create a new site, click Add Base.</td>
<td></td>
</tr>
<tr>
<td>c. To create a sub-location, right-click a location and select New [Element].</td>
<td></td>
</tr>
<tr>
<td>d. To change the properties for an element, right-click a location and select Edit.</td>
<td></td>
</tr>
<tr>
<td>Tip You can create any combination of location elements. Door configurations can be assigned to any level of the hierarchical tree.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** Open the Hardware module.

a. Select Hardware from the Doors menu.

b. Select Device from the View menu, if necessary.

Note See Viewing Doors and Devices in the Hardware View, page 5-3 for more information.

**Step 3** Add a Gateway to Cisco PAM.

a. Right-click Access Gateway Driver.

b. Select New Gateway Controller.

Note Gateways can also be automatically added to the configuration. See Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2.
**Step 4**
Select a Door template.

a. Select **Yes**.

b. Select a **Template**.

c. Click **Next**.

**Note**    Cisco PAM includes sample templates. To create or modify templates, see **Understanding Door Configurations and Templates, page 5-20** and Chapter 7, “Configuring Door and Device Templates”.

**Step 5**
Enter the name, serial number, and location of the Gateway module.

a. **Name**: enter a descriptive name to identify the Gateway module.

b. **Serial Number**: the serial number is unique and cannot be changed. See **Locating Serial Numbers, page 5-36**.

c. **Location**: the assigned location of the module. See **Viewing Doors and Devices by Location, page 5-5**.

**Note**    The Time Zone and Daylight Savings setting are not configurable if defined by the template.

d. Click **Next**.
Chapter 6  Configuring Doors

Step 6  Edit or enter the properties for each module in the Gateway template.

a. Select a module from the list (Gateway, Reader, Input, or Output).

b. Click Edit.

c. Enter a descriptive name for the device.

d. (Expansion modules only) Enter the serial number for the module. The Gateway serial number was entered in the previous screen (Step 5).

e. (Reader module only) Select the Reader connection mode: one door or two door configuration.

f. Click Update.

g. Repeat these steps for each module in the list.

h. Click Next.

Step 7  (Optional) If door configurations are included in the Gateway template, assign each door to a location.

Note  If door configurations are not included in the Gateway template, complete these instructions, and continue to Adding Doors Using Door Templates, page 6-7.

a. Select a door template from the list.

b. Click Edit.

c. Enter the following information:

   - Door Name: enter a descriptive name for the door.

   - Door Location: select a location for the door (see Viewing Doors and Devices by Location, page 5-5).

d. Click Update.

e. Repeat these steps for each available door.

f. Click Finish to create the door configuration(s).
## Chapter 6: Configuring Doors

### Step 8
(Conditional) Modify the door and device properties, if necessary.

- **a.** Select **Location & Doors** from the **Doors** menu.
- **b.** Navigate to the door by expanding the locations as necessary (click on the box next to an icon to expand or collapse the locations). The door is located under the location selected when adding the door (see **Step 7**).
- **c.** Double click the door or device to open the properties window (or right-click the door and select **Edit**).

To override a template settings, uncheck the Default box to activate the field.

For more information, see the following:

- Chapter 5, “Understanding Door Configuration”
- Door Configuration Properties, page 7-25
- Device Configuration Properties, page 7-27

**Tip** You can also modify doors using the Hardware module. Doors are listed under the Logical Device driver, or in the Hierarchical Locations view.

### To do this

<table>
<thead>
<tr>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image 1" /> <img src="image2.png" alt="Image 2" /></td>
</tr>
</tbody>
</table>
Step 9

Select **Apply Configuration Changes** on the Gateway Driver or on a specific Gateway.

- Right-click the **Access GW Driver** and select **Apply Configuration Changes** to download configuration changes for all Gateways.

  or

- Right-click on a specific **Gateway Controller** and select **Apply Configuration Changes** to download configuration changes for a single Gateway.

  **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. For more information, see **Applying Configuration Changes**, page 6-17

Step 10

(Optional) Continue to **Adding Doors Using Door Templates**, page 6-7

---

**Related Documentation**

For more information, see the following:

- Chapter 5, “Understanding Door Configuration”
- Chapter 7, “Configuring Door and Device Templates”
Adding Doors Using Door Templates

Complete the following instructions to add a door using a door template. You can accept the default configurations included in the door template, or override most settings.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the Gateway for the door configuration exists in the Hardware module. If the Gateway is not already configured, use one of the following methods:&lt;ul&gt;&lt;li&gt;Adding Doors Using Door Templates, page 6-7&lt;/li&gt;&lt;li&gt;Creating Custom Gateway Configurations and Templates, page 7-2.&lt;/li&gt;&lt;/ul&gt;Note: See also Provisioned (Pre-Populated) vs. Discovered Gateway Configurations, page 5-2.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a new door: &lt;ul&gt;&lt;li&gt;a. Select Locations &amp; Doors from the Doors menu.&lt;/li&gt;&lt;li&gt;b. Right-click a location and select New Door.&lt;/li&gt;&lt;/ul&gt;Note: If the location does not exist, refer to Creating the Location Map, page 5-6 for more information. Tip: You can also create a door in the Hardware module. Right click on the Logical Driver and select New Door.</td>
</tr>
</tbody>
</table>
| **Step 3** | Enter the General settings:<ul><li>Door name: enter a descriptive name for the door configuration.</li><li>Door Template: select the door template that contains the correct set of door devices. See Configuring Door Templates, page 7-7 for more information.</li><li>Gateway: select the Gateway used for the door configuration. The devices in the door template are assigned to the Gateway interfaces.</li></ul>
### Configuring Doors

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> Select a location for the door.</td>
<td><img src="image" alt="Display" /></td>
</tr>
<tr>
<td>a. Select the <strong>Location</strong> sub-menu.</td>
<td><img src="image" alt="Display" /></td>
</tr>
<tr>
<td>b. In the Hierarchical Location field, do one of the following:</td>
<td><img src="image" alt="Display" /></td>
</tr>
<tr>
<td>• Click the drop down menu to select the new location from a list.</td>
<td><img src="image" alt="Display" /></td>
</tr>
<tr>
<td>• Click <strong>Set</strong> to open a pop-up window and select the location from a hierarchical map (see example screen).</td>
<td><img src="image" alt="Display" /></td>
</tr>
<tr>
<td>• Click <strong>Clear</strong> to remove the setting. The door will appear in the Unassigned category.</td>
<td><img src="image" alt="Display" /></td>
</tr>
<tr>
<td>To do this</td>
<td>Use this display</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Step 5</strong> Associate each device with a specific interface on a Gateway module. If the Gateway includes expansion modules, you can also choose an interface from a Reader, Input, or Output module.</td>
<td>![Diagram 1]</td>
</tr>
<tr>
<td>a. Select the <strong>Associate Devices</strong> sub-menu.</td>
<td></td>
</tr>
<tr>
<td>b. Highlight a device (such as Reader) and click <strong>Associate Device</strong>.</td>
<td></td>
</tr>
<tr>
<td>c. In the <strong>Select Device</strong> window, click the <strong>New</strong> button.</td>
<td></td>
</tr>
<tr>
<td>d. In the <strong>New Device</strong> window, select a module and module interface for the device.</td>
<td>![Diagram 2]</td>
</tr>
<tr>
<td><strong>Note</strong> The Gateway module is m00. If expansion modules such as the Reader, Input, or Output module are configured on the Gateway, a selection for each relevant module is also available.</td>
<td>![Diagram 3]</td>
</tr>
<tr>
<td>e. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
## To do this

### Step 6
Accept or modify the device settings.

The configuration for the device is pre-defined by the door template. You can accept the default settings, or modify the configuration as necessary. Changes apply only to the current device and do not affect the template.

- a. Select the **Properties** sub-menu.
- b. (Optional) To change the default settings for a field, deselect the Default check box. Click **Save and Close** to save the configuration.

See **Device Configuration Properties**, page 7-27 for more information.

<table>
<thead>
<tr>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Add Reader" /></td>
</tr>
</tbody>
</table>

### Step 7
Select the interface for the device in the **Select Device** window:

- a. Highlight the interface from the list in the **Available Device** field. This list includes the available unused ports from the Gateway and any expansion modules attached to the Gateway.
- b. Click **OK** to save the change and complete the device association.

<table>
<thead>
<tr>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image2.png" alt="Select Device" /></td>
</tr>
</tbody>
</table>

### Step 8
Repeat Step 5 to Step 7 to associate each device to an interface.

**Tip** When all devices are associated with an interface, a **Name** appears for each device.

<table>
<thead>
<tr>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3.png" alt="Add Door" /></td>
</tr>
</tbody>
</table>
Step 9  
(Optional) Modify the Properties for the door.

a. Click the Properties sub-menu.

b. To change the default settings for a field, 
   deselect the Default check box.

For more information see the following:

- Chapter 5, “Understanding Door 
  Configuration”
- Door Configuration Properties, page 7-25

Step 10  
(Optional) Modify the LED Usage Profiles for the 
    door.

a. Click the Usage Profiles sub-menu.

b. To change the default settings for a field, 
   deselect the Default check box.

See Configuring Reader LED Profiles, page 7-21 
for more information.
### Step 11
(Optional) Modify the Facility Codes for the credential templates used in the door configuration:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Click the <strong>Facility Code Information</strong> sub-menu.</td>
<td><img src="image" alt="Facility Code Information" /></td>
</tr>
<tr>
<td>b. Uncheck the Default box to activate the configuration fields.</td>
<td></td>
</tr>
<tr>
<td>c. Click <strong>Add</strong> to add a credential template to the list.</td>
<td></td>
</tr>
<tr>
<td>d. Select a credential template from the drop-down menu.</td>
<td></td>
</tr>
<tr>
<td>e. Enter the Facility Codes. Separate codes with a comma (,).</td>
<td></td>
</tr>
<tr>
<td>f. Click <strong>Save</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**To Edit a credential template:**

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Highlight the template in the Credential Template list box.</td>
<td><img src="image" alt="Credential Template List" /></td>
</tr>
<tr>
<td>b. Click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>c. Select a credential template from the drop-down menu.</td>
<td></td>
</tr>
<tr>
<td>d. Enter the Facility Codes. Separate codes with a comma (,).</td>
<td></td>
</tr>
</tbody>
</table>

**To delete a credential template:**

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Highlight the template in the Credential Template list box.</td>
<td><img src="image" alt="Credential Template List" /></td>
</tr>
<tr>
<td>b. Click <strong>Delete</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

See [Configuring Credential Templates, page 7-17](#) for more information.
## Configuring Doors

### Step 12
(Optional) Modify the Duress Specifications for the door.

- a. Click the **Duress Specification** sub-menu.
- b. Uncheck the Default box to activate the configuration fields.
- c. Click **Add** to add an alarm to the list.
- d. Select an Alarm from the drop-down menu.
- e. Enter the Code.
- f. Click **Save**.

To Edit an alarm:

- a. Highlight the alarm in the list box.
- b. Click **Edit**.
- c. Select an alarm from the drop-down menu.
- d. Enter the Code.

To Delete an alarm:

- a. Highlight the alarm in the list box.
- b. Click **Delete**.

### Step 13
Click **Save and Close** to save the changes and return to the main window.

The door configuration is displayed as a child of the selected location.

**Note** The door is also listed under the Logical Driver in the Hardware module.

### Step 14
Apply the door configuration changes.

In the Locations & Doors module, right-click a location and select **Apply Configuration Changes**. Only Gateways in the Up state are updated.

For more information, see Applying Configuration Changes, page 6-17
Modifying Door Configurations

This section includes instructions to modify an existing door or device configuration using the following methods:

- Modifying Door and Device Templates, page 6-14
- Modifying Devices in the Hardware Device View, page 6-14
- Modifying Devices in Hardware Location View, page 6-15
- Modifying Devices in the Locations & Doors Module, page 6-16

Modifying Door and Device Templates

For instructions to modify templates, see Chapter 7, “Configuring Door and Device Templates”.

Modifying Devices in the Hardware Device View

To manually revise the properties for a Gateway, expansion module, or other device, do the following:

Step 1 Select Hardware from the Doors menu.

Step 2 Expand the hardware tree, right-click on the device name, and select Edit, as shown in Figure 6-1. You can also double-click the device name to open the edit window.

Step 3 Click Properties in the device window and edit the settings as necessary. To override the template settings, deselect the Default checkbox to activate the field. For field descriptions, see Door Configuration Properties, page 7-25 and Device Configuration Properties, page 7-27.

Step 4 Download the configuration changes to the Gateway. Changes do not take effect until downloaded. See Applying Configuration Changes, page 6-17.
Chapter 6      Configuring Doors

Modifying Door Configurations

![Figure 6-1  Edit Menu for a Device in the Hardware Device View](image)

**Step 1**  In the Hardware module, select **Hierarchical Location** from the View menu.

**Step 2**  Expand the location tree to display the door configuration.

**Step 3**  Right-click on the device name and select **Edit**, as shown in Figure 6-2. You can also double-click the door to open the edit window.

**Step 4**  Select a sub-menu and edit the settings as necessary. To override the template properties, deselect the Default checkbox to activate the field.

**Step 5**  Download the configuration changes. See **Applying Configuration Changes**, page 6-17.

---

**Modifying Devices in Hardware Location View**

You can edit door configurations in the Hardware location view, but you cannot edit device properties or the location map.

**Step 1**  In the Hardware module, select **Hierarchical Location** from the View menu.

**Step 2**  Expand the location tree to display the door configuration.

**Step 3**  Right-click on the device name and select **Edit**, as shown in Figure 6-2. You can also double-click the door to open the edit window.

**Step 4**  Select a sub-menu and edit the settings as necessary. To override the template properties, deselect the Default checkbox to activate the field.

**Step 5**  Download the configuration changes. See **Applying Configuration Changes**, page 6-17.

![Figure 6-2  Edit Menu for a Door in the Hardware Location View](image)
Modifying Devices in the Locations & Doors Module

In the Locations & Doors module, you can edit all attributes of a door configuration, including device properties and the location map.

For instructions to modify the location map, see Creating the Location Map, page 5-6.

Step 1
In the Locations & Doors module, expand the location tree to display the door configuration or a specific device.

Step 2
Right-click on the door or device name and select Edit, as shown in Figure 6-3.

Tip
You can also double-click a door or device to open the edit window.

Step 3
Select a sub-menu and edit the settings as necessary. To override the template properties, deselect the Default checkbox to activate the field.

Step 4
Download the configuration changes. See Applying Configuration Changes, page 6-17.

Tip
The names of all hardware elements are editable, including Drivers, Gateways, expansion modules, and door devices.
Applying Configuration Changes

Changes made to a door or device configuration in Cisco PAM are inactive until applied to the Gateway module. You can apply the configuration changes to a specific Gateway, to all Gateways, or to all Gateways in a location. Applying a configuration downloads the revised configuration file to the Gateway.

Gateways must be in the Up state, signified by a green triangle in the icon. A dark green triangle signifies that the Gateway has configuration changes that have not been applied (downloaded).

This section includes the following information.
- Applying Configuration Changes to Gateways, page 6-17
- Configuration Management in Provisioned vs. Discovered Configurations, page 6-18

Applying Configuration Changes to Gateways

You can download the configuration to Gateways using either the Hardware or Locations & Doors modules.

Applying Configuration Changes in the Hardware Module

Select Apply Configuration Changes on the Gateway Driver or on a specific Gateway.

- Right-click the Access GW Driver and select Apply Configuration Changes to download configuration changes for all Gateways.

or

- Right-click on a specific Gateway Controller and select Apply Configuration Changes to download configuration changes for a single Gateway.

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. See Understanding Device Status Colors, page 5-12.
Applying Configuration Changes in the Locations & Doors Module

Select **Apply Configuration Changes** on the affected Gateway or on a Location.

**Specific Gateway**

- Select **Gateway Controllers** from the View menu to display the Gateways.
- Right-click a Gateway icon and select **Apply Configuration Changes** to download the configuration for a single device.

**Multiple Gateways**

- Right-click a location icon.
- 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. See **Understanding Device Status Colors**, page 5-12.

Configuration Management in Provisioned vs. Discovered Configurations

- In a Provisioned configuration, the configuration is entered before the Gateway module is brought online and the configuration is automatically downloaded when the Gateway is added to the network. Any subsequent configuration changes must be downloaded using one of the methods described in this section.
- In a Discovered configuration, the Gateway is added to the network before a configuration is created. Cisco PAM automatically creates a basic configuration containing the serial numbers of the Gateway and any expansion modules. Any subsequent configuration changes must be downloaded using one of the methods described in this section.
- If a Gateway power-cycles or is disconnected and reconnected to the network, the last configuration applied to the module will automatically be downloaded when the module comes online.

**Note** See **Provisioned (Pre-Populated) vs. Discovered Gateway Configurations**, page 5-2 for more information.
Disabling or Deleting a Device or Door

Disabling a device or door configuration deactivates the item, but does not remove it from the Cisco PAM configuration. This allows you to remove the device or door from the active configuration without deleting it entirely. The device or door can be re-enabled, if necessary, and the configuration, events, logs and alarms associated with the device or door are retained.

**Note**

Interface and drivers (such as the Access GW Driver and Logical Driver) cannot be disabled.

When you delete a device or door, all configurations and other information, including events and logs, are also permanently deleted and cannot be recovered. Only deactivated devices or doors can be deleted. Cisco Systems does not recommend deleting devices since clearing a large number of events can be time and processor intensive.

This section includes the following information:

- Disabling a Device or Door, page 6-19
- Deleting Devices and Doors, page 6-20
- Enabling a Device or Door, page 6-23

Disabling a Device or Door

To disable a device or door, right-click the item and select **Disable** from the drop down menu.

**Note**

Changes are not applied until you download the revised configuration to the Gateways.

**Step 1**

Select either **Hardware** or **Locations & Doors** from the Doors menu.

**Step 2**

Right-click a Gateway, door configuration, or other device, and select **Disable** *(Figure 6-4).*

*Figure 6-4  Disabling a Device Using the Hardware Module*
• **Disabling a device**: removes the Gateway association and may disable the door configuration. A confirmation message appears describing the impact of disabling the device.

• **Disabling a Gateway**: disables all associated devices and door configurations. A confirmation message appears describing the impact of the action.

• **Disabling a door configuration**: a confirmation window allows you to select the associated devices to be disabled, as shown in Figure 6-5. Select the devices to be disabled, or check the box for Select All, and then click Yes.

![Figure 6-5 Confirmation Warning When Disabling a Door Configuration](image)

**Step 3** Download the configuration changes to the Gateway. Changes do not take effect until downloaded. See **Applying Configuration Changes**, page 6-17.

**Step 4** (Optional) To delete a device, Gateway or door configuration, see **Deleting Devices and Doors**, page 6-20.

To view disabled devices, select **All Devices** from the **Filter** menu.

### Deleting Devices and Doors

When a device is deleted, the device is permanently removed from the Cisco PAM configuration. All events associated with the device are also permanently deleted. Neither the device or the events can be restored. This is different than disabling a device. When a device is disabled, it remains in the configuration and can be re-enabled at a later time.

**Note** Cisco Systems does not recommend deleting devices since clearing a large number of events can be time and processor intensive.

**Tip** To delete a device or door, you must first enable the delete functions and then disable the device or door.

This section includes the following information.

• **Enabling the Delete Options**, page 6-21

• **Deleting a Device**, page 6-22
Enabling the Delete Options

Step 1 Select **System Configuration** from the Admin menu.

Step 2 Select the **Miscellaneous** sub-menu, as shown in Figure 6-6

![Figure 6-6 Device Delete Options in The Admin Module: System Configuration](image)

Step 3 Select or deselect one of the following:

- **Allow deletion of items that normally may only be disabled**: Adds the *Delete* option to device and door right-click menus. Devices can be deleted only if they were previously disabled, are not referred to by another object, and if have no events or alarms. Deleting a device or door permanently removes the item from the configuration.

- **Allow deletion of devices with events**: Adds the *Delete* option to device and door right-click menus. This option deletes the device and any associated events. Items with active alarms cannot be deleted. Devices and doors can be deleted only if they were previously disabled and are not referred to by another object.

**Note** Deleting a device may temporarily impact system performance while the associated events are also deleted. Do not delete devices and doors unless necessary.

Step 4 Click *Save* to save the changes.

Step 5 Exit all Cisco PAM windows and restart the application to activate the changes. The *Delete* menu does not appear in Cisco PAM until the application is closed and re-opened.
Disabling or Deleting a Device or Door

Deleting a Device

To delete a device, do the following:

**Step 1** Enable the Delete functions, as described in Enabling the Delete Options, page 6-21.

**Step 2** Disable the device, as described in Disabling a Device or Door, page 6-19.

**Step 3** Select All Devices from the Filter menu to display the disabled device(s).

**Step 4** Right-click the device and select Delete.

**Step 5** Select Yes to confirm.

**Step 6** Download the changes to the Gateway, as described in Applying Configuration Changes, page 6-17.

Deleting a Gateway Controller

To delete a Gateway Controller, do the following:

**Step 1** Enable the Delete functions, as described in Enabling the Delete Options, page 6-21.

**Step 2** Disable all devices in all doors associated with the Controller, as described in Disabling a Device or Door, page 6-19.

**Step 3** Select All Devices from the Filter menu to display the disabled device(s).

**Step 4** Delete the Gateway Controller by right-clicking the Controller and selecting Delete.

**Step 5** Select Yes to confirm.

**Step 6** Download the changes to the Gateway, as described in Applying Configuration Changes, page 6-17.
Enabling a Device or Door

When a device is disabled, the door is also disabled. To re-enable a door and device, re-associate all devices and then enable the door, as described in the following example.

Disable and Enable a Device and Door: Example

The following example describes how to disable and then re-enable a device:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Disable a device:</strong></td>
</tr>
<tr>
<td>1.</td>
<td>Right-click the device and select <strong>Disable</strong>. A confirmation message appears.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Yes</strong> to disable the device. The door is also disabled.</td>
</tr>
</tbody>
</table>
# Enabling a Device or Door

**Step 2**  
Re-enable the door.

**Note** To re-enable a door, you must reassociate the device with the door.

- Select **All Devices** from the Filter menu to display the disabled device(s).
- Right-click on the door and select **Edit** to open the edit window.
- Select the **Associate Devices** sub-menu, as shown in the example to the right.
- Highlight a device (such as Reader) and click **Associate Device**.
- In the **Select Device** window, click the **New** button.
- In the **New Device** window, select a module and module interface for the device.

**Note** The default Gateway module name is `m00`.

- Click **OK**.

## To do this

<table>
<thead>
<tr>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Add Door" /></td>
</tr>
<tr>
<td><img src="image2.png" alt="Select Device" /></td>
</tr>
<tr>
<td><img src="image3.png" alt="Input New Device" /></td>
</tr>
</tbody>
</table>
### Enabling a Device or Door

<table>
<thead>
<tr>
<th>Step</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Accept or modify the device settings. Click <strong>Save and Close</strong> to save the configuration.</td>
<td><img src="example.png" alt="Image 1" /></td>
</tr>
</tbody>
</table>
| Step 4 | Select the interface for the device in the **Select Device** window:  
  a. Highlight the interface from the list in the **Available Device** field. This list includes the available unused ports from the Gateway and any expansion modules attached to the Gateway.  
  b. Click **OK** to save the change and complete the device association. | ![Image 2](example.png) |
| Step 5 | Associate additional devices, or save the changes:  
  a. Verify that an entry appears in the **Name** column for each device.  
  b. Associate any additional devices that do not appear with a Name.  
  c. Click **Save and Close** to save the configuration and re-enable the device. | ![Image 3](example.png) |
### Step 6
Re-enable the door.

**Note** The device should appear again under the door.

Right-click the door name, and select **Enable**.

### Step 7
Apply the door configuration changes.

Right-click a location or Gateway and select **Apply Configuration Changes**. Only Gateways in the Up state are updated.

For more information, see **Applying Configuration Changes**, page 6-17.
Cloning a Gateway Configuration

Cloning a Gateway creates an exact copy of a Gateway configuration, including any attached expansion modules, devices, or door configurations. Only the names, locations, and serial numbers of the devices and doors are changed in the clone. A Gateway clone is an independent copy, and is used to configure one other Gateway module. Changes to the original Gateway or to the clone Gateway do not effect each other.

To create a Gateway clone, do the following:

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

Step 2 Right-click a Gateway Controller and select Clone Gateway.

Step 3 Enter the names, serial numbers, and locations for the clone Gateway. For expansion modules, note the type of expansion module that each serial number is assigned to, and match it to the same type of module for the clone configuration.

Step 4 (Optional) Click Clone all module names to use the source names for the clone configuration.

Step 5 Click OK.

Step 6 Right-click the Gateway icon and select Reload Gateway Configuration. This command downloads the full configuration and replaces the existing file on the specified Gateway. The Gateway must be installed and in the Up state, or the reload will fail.

Step 7 Add doors or revise the configuration as necessary. See Configuring Doors, page 6-2 for more information.

Tip To create a template from a Gateway configuration, see Creating Custom Gateway Configurations and Templates, page 7-2.
Configuring Device Groups

Use device groups to create sets of devices for use in other configuration menus such as Event Policies (Modifying Default Event Policies, page 10-28) and Access Policies (Configuring Access Policies, page 9-2).

For example, a device group for all lobby doors can be created, and then specified in an access policy. Users assigned to that access policy will only have access to doors in that device group.

To configure device groups, do the following:

---

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

The main window opens, as shown in Figure 6-7.

*Figure 6-7  Device Groups Main Window*

---

**Step 2**
Add or edit a device group.

- To add a new device group, click Add.
- To modify an existing record, select the record and click Edit, or double-click the entry.

**Note**
To remove a device group, you must first remove any configurations for that group in the Access Policy or Event Policy modules. Once the associations are removed, select the entry and click Delete. If you attempt to remove a device group that is still in use, a pop-up message appears with a summary of the access and event policies that are associated with the group.
Step 3  In the detail window (Figure 6-8), enter a Name for the device group. For example: Employee Doors.

![Device Group Detail Window](image)

Figure 6-8  Device Group Detail Window

Step 4  Select the device Type.
For example: Door, Gateway, Module, Reader, etc.
When selected, the Group Members field displays the devices for that device type.

Step 5  Select the devices to include in the group. For example, in Figure 6-9 the lobby doors are selected to create a lobby door group.

Tip
- Devices can belong to multiple groups.
- Check the site name to select all the devices for that site.
- Click Uncheck All to clear the selections.
Figure 6-9  Door Groups: Choose Devices Window

Step 6  Click **Save and Close** to save the changes and exit the Device Group detail window. The new door group appears in the main window (Figure 6-7).
Replacing a Gateway or Expansion Module

To replace a Gateway or expansion module with a new device, complete the following instructions.

**Note**
The replacement module must be the same as the old module, and all device connections must be the same. All configurations and properties remain the same.

**Step 1**
Physically remove the old device. Cisco PAM automatically detects the removal and disables the device configuration.

**Step 2**
In the **Hardware** module, select **All Devices** from the **Filter** menu to display the disabled device.

**Step 3**
Right-click the device icon and select **Replace Gateway** or **Replace Module**. These commands are enabled only after a device is disconnected.

**Step 4**
Enter the serial ID (number) of the replacement device and click **OK**.

**Step 5**
Physically install the replacement Gateway or expansion module.

**Tip**
Connect expansion modules to the same Gateway interface. The Gateway automatically recognizes the new module, and enables the device in Cisco PAM.

**Step 6**
Right-click the Gateway icon and select **Reload Gateway Configuration**. This command downloads the correct (full) configuration to the Gateway.

Changing Gateway Passwords

You can change the password for one or more Gateways in the **Hardware** module, or the **Locations & Doors** module.

**Step 1**
Display the Gateways:
- Select **Locations & Doors** from the **Doors** menu and select **Gateway Controllers** from the **View** menu.
  - or
- Select **Hardware** from the **Doors** menu and expand the Access GW Driver device tree.

**Step 2**
Change the password for one or more Gateways:
- To change the password for a single device, right-click a Gateway icon and select **Reset Gateway Password**.
To change the password for a multiple devices, right-click the location icon or the Access GW Driver and select **Reset Gateway Password**. Changing the password for a location affects only the Gateways at that location. Changing the password for the driver affects all the Gateways in the system.

See Figure 6-10 and Figure 6-11 for examples to change the Gateway passwords.

**Figure 6-10  Reset Gateway Password**

![Gateway Password Window]

**Figure 6-11  Reset Gateway Password**

![Gateway Password Window]

**Step 3** (Optional) In the Reset Gateway Password window (Figure 6-12 on page 6-33), click **Preview** to view a list of Gateways. Gateways must be in the **Up** or **Down** state. If a Gateway is in the **Unknown** state, the device is displayed in red and the password is not changed.

**Step 4** Enter a new password and click **OK** (Figure 6-12).
Step 5 Verify the status of the change:

- In the Locations & Doors module, select a location. The command status is displayed under Extended Status in the lower right of the screen (see Figure 6-10 on page 6-32).
- In the Hardware module, select the Access GW Driver. Select the Command Status tab under Extended Status in the lower right of the screen (see Figure 6-10 on page 6-32).

Tip To change Gateway settings using a direct PC connection, you must connect a PC to the module and enter a password, as described in the Cisco Physical Access Gateway User Guide.
Device and Driver Commands in the Hardware Device View

To access the following commands, right-click on the driver or module icon in the Hardware module (select Hardware from the Doors menu).

- Access GW Driver Commands, page 6-34
- Gateway Controller Commands, page 6-35
- Reader Module Commands, page 6-37
- Input and Output Module Commands, page 6-37
- Logical Driver Commands, page 6-38

Access GW Driver Commands

Table 6-1   Access GW Driver Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Configuration Changes</td>
<td>Downloads configuration changes to all Gateway modules. Changes made in Cisco PAM are inactive until applied with this command. See Applying Configuration Changes, page 6-17.</td>
</tr>
<tr>
<td>Apply Credential Changes</td>
<td>Downloads credential changes to all Gateway modules. Credential changes made in Cisco PAM are downloaded every 60 minutes by default, and are inactive until then. Use the Apply Credential Changes command to download the credential configuration to all Gateways immediately. See Downloading Credential Changes to the Gateway Modules, page 8-10.</td>
</tr>
<tr>
<td>Reset Gateway Password</td>
<td>Resets the password on all configured Gateways. See Changing Gateway Passwords, page 6-31.</td>
</tr>
<tr>
<td>Bulk Image Upgrade</td>
<td>Downloads a firmware image to all Gateway modules. See Upgrading Gateway Firmware Images Using Cisco PAM, page B-18.</td>
</tr>
<tr>
<td>Run System Sanity Report</td>
<td>Creates a snapshot of potential inconsistencies in the system. See Generating a System Sanity Report, page 5-16.</td>
</tr>
<tr>
<td>View Recent Events</td>
<td>View a list of recent events for all Gateways. See Viewing the Recent Events for a Device, Driver, or Location, page 5-14.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit window to revise the driver properties.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables all Gateways, attached devices, and door configurations. See Disabling or Deleting a Device or Door, page 6-19. Disabled Devices can be re-enabled.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently removes the Gateways and attached devices from the configuration. See Disabling or Deleting a Device or Door, page 6-19.</td>
</tr>
</tbody>
</table>
### Table 6-1  Access GW Driver Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Device Status</td>
<td>Opens a new window containing the Status and Extended Status information. See Viewing Device and Door Status, page 5-9.</td>
</tr>
<tr>
<td>Show in Graphic Map Editor</td>
<td>The Graphic Maps Editor module allows operators to add facility maps, plot and organize devices for use in the Graphic Map Viewer module. See Graphic Map Editor, page 10-42.</td>
</tr>
</tbody>
</table>

### Gateway Controller Commands

### Table 6-2  Gateway Controller Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Configuration Changes</td>
<td>Downloads configuration changes to the specified Gateway module. Changes made in Cisco PAM are inactive until applied with this command.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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. For more information, see Applying Configuration Changes, page 6-17.</td>
</tr>
<tr>
<td>Reload Gateway Configuration</td>
<td>Downloads the full configuration and replaces the existing file on the specified Gateway. The Gateway must be installed and in the Up state, or the reload will fail.</td>
</tr>
</tbody>
</table>
| File Manager                   | Provides info of various files available on the Gateway:  
   - **Images**: Set of firmware images available on the Gateway including status. See Upgrading Gateway Firmware Images Using Cisco PAM, page B-18 for more info.  
   - **Core Files**: Core files for any core dumps that occurred on the Gateway.  
   - **Log File**: List of debug log files.  
   - **Technical Summary**: Technical data to assist in debugging issues.  
   **Note**: Each screen also provides options to download or upload the files. |
| Save As Gateway Template       | Saves the Gateway configuration as a template that can be used to configure additional devices. See Creating Custom Gateway Configurations and Templates, page 7-2 and Gateway Templates, page 5-23. |
| Reset Gateway                  | Performs a soft reset of the Gateway. See the Cisco Physical Access Gateway User Guide.                                                    |
### Table 6-2  Gateway Controller Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Gateway Address</td>
<td>Replaces the Gateway Network configuration.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Gateway network settings can also be configured using a direct connection to the Gateway. See the <em>Cisco Physical Access Gateway User Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>If this command is used to enter the Gateway Network configuration, all settings on the Gateway are replaced. You <strong>cannot</strong> use this command to modify only selected parameters.</td>
</tr>
<tr>
<td></td>
<td>To view the current settings, select the Gateway in the Hardware module. In the Extended Status screen (bottom right window), select the <strong>Gateway Network Address</strong> tab.</td>
</tr>
<tr>
<td>Format Gateway Flash</td>
<td>Erases and formats the Gateway flash memory.</td>
</tr>
<tr>
<td>Replace Gateway</td>
<td>Replaces the current Gateway with new Gateway device. This command is active only when the device is disconnected from Cisco PAM (Unknown State). The command is used to replace a faulty device. See Replacing a Gateway or Expansion Module, page 6-31.</td>
</tr>
<tr>
<td>Reset Gateway Password</td>
<td>Resets the password for the selected Gateway device. You can also reset the passwords for multiple Gateways. See Changing Gateway Passwords, page 6-31.</td>
</tr>
<tr>
<td>Download All Credentials</td>
<td>Downloads all credentials to the Gateway to ensure all required data is correct. This command should be used only if a problem exists.</td>
</tr>
<tr>
<td>Credential Look up</td>
<td>Search for the credentials on a Gateway.</td>
</tr>
<tr>
<td>View Recent Events</td>
<td>View a list of recent events for the Gateway. See Viewing the Recent Events for a Device, Driver, or Location, page 5-14.</td>
</tr>
<tr>
<td>New Module</td>
<td>Adds a new expansion module to the Gateway configuration.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit window to revise the device properties.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables the device and all attached devices. Also disables any door configurations. See Disabling or Deleting a Device or Door, page 6-19. Disabled Devices can be re-enabled.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Device or Door, page 6-19.</td>
</tr>
<tr>
<td>View Device Status</td>
<td>Opens a new window containing the Status and Extended Status information.</td>
</tr>
<tr>
<td>Show in Graphic Map Editor</td>
<td>The <strong>Graphic Maps Editor</strong> module allows operators to add facility maps, plot and organize devices for use in the <strong>Graphic Map Viewer</strong> module. See Graphic Map Editor, page 10-42.</td>
</tr>
</tbody>
</table>
Reader Module Commands

Table 6-3  Reader Module (Module 00) Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Module</td>
<td>Resets the device.</td>
</tr>
<tr>
<td>Squelch</td>
<td>Suppresses any events from this module. Events are not reported or saved.</td>
</tr>
<tr>
<td>Unsquelch</td>
<td>Undo squelch. Events are reported and saved.</td>
</tr>
<tr>
<td>View Recent Events</td>
<td>View a list of recent events for the module. See Viewing the Recent Events for a Device, Driver, or Location, page 5-14.</td>
</tr>
<tr>
<td>Replace Module</td>
<td>Replaces the current module with new device. This command is active only when the device is disconnected from Cisco PAM (Unknown State). See Replacing a Gateway or Expansion Module, page 6-31.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit window to revise the device properties.</td>
</tr>
<tr>
<td>Edit Reader Connection Mode</td>
<td>Defines if the module supports connections for one or two readers. See the Cisco Physical Access Gateway User Guide for more information on reader connections.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables the device and all attached devices. Also disables referenced door configurations. See Disabling or Deleting a Device or Door, page 6-19. Disabled Devices can be re-enabled.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Device or Door, page 6-19.</td>
</tr>
<tr>
<td>View Device Status</td>
<td>Opens a new window containing the Status and Extended Status information.</td>
</tr>
<tr>
<td>Show in Graphic Map Editor</td>
<td>The Graphic Maps Editor module allows operators to add facility maps, plot and organize devices for use in the Graphic Map Viewer module. See Graphic Map Editor, page 10-42.</td>
</tr>
</tbody>
</table>

Input and Output Module Commands

Table 6-4  Input and Output Module Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Module</td>
<td>Resets the device.</td>
</tr>
<tr>
<td>Squelch</td>
<td>Suppresses any events from this module. Events are not reported or saved.</td>
</tr>
<tr>
<td>Unsquelch</td>
<td>Undo squelch. Events are reported and saved.</td>
</tr>
<tr>
<td>Replace Module</td>
<td>Replaces the current device with new device. This command is active only when the device is disconnected from Cisco PAM (Unknown State). The command is used to replace a faulty device. See Replacing a Gateway or Expansion Module, page 6-31.</td>
</tr>
</tbody>
</table>
Logical Driver Commands

To access the following commands, right-click on the Logical Driver icon in the Hardware view.

Table 6-5 Logical Driver Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Recent Events</td>
<td>View a list of recent events for the configured doors. See Viewing the Recent Events for a Device, Driver, or Location, page 5-14.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens the Edit window to revise the driver properties.</td>
</tr>
<tr>
<td>Disable</td>
<td>Enables the device and all attached devices. Also disables referenced door configurations. See Disabling or Deleting a Device or Door, page 6-19. Disabled Devices can be re-enabled.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently removes the device and all attached devices from the configuration. See Disabling or Deleting a Device or Door, page 6-19.</td>
</tr>
<tr>
<td>View Device Status</td>
<td>Opens a new window containing the Status and Extended Status information.</td>
</tr>
<tr>
<td>Show in Graphic Map Editor</td>
<td>The Graphic Maps Editor module allows operators to add facility maps, plot and organize devices for use in the Graphic Map Viewer module. See Graphic Map Editor, page 10-42.</td>
</tr>
</tbody>
</table>
Door Modes and Commands

Door Modes

A door mode indicates the state of the door, including one of the following:

- **Open**: The door is physically held open. The lock is in Unlocked state, the door sensor is dis-engaged. When door is in Open mode, and a badge is presented to a reader, the badge data is read but may not be validated.

- **Close**: The door is physically closed. The lock is in Unlocked state and the door sensor is engaged, indicating door is closed. When the door is in Close mode, and a badge is presented, the badge data is read but may not be validated.

- **Lock**: The door is physically closed and the lock is in Locked state. The Door Sensor is engaged. When the door is in Lock mode, and a badge is presented, the badge data is read and validated: if access is granted the lock is opened, access is denied if the badge is invalid.

- **Secure**: The door is locked and the deadbolt is applied. The deadbolt remains in place until issue a command to change the door mode (such as **Reset Door Mode**). See Door Commands, page 6-39 for more information.

**Tip**

For more information, see Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 5-25.

Door Commands

The following commands are available when you right-click a door configuration in the Device or Locations view (available in either Hardware or Doors & Locations).

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Access</td>
<td>Grants access to the door.</td>
</tr>
<tr>
<td>Grant Access ADA</td>
<td>Grants access to a door, and applies the ADA settings, such as the amount of time the door is held open, or use of a mechanical swing device. See Door Configuration Properties, page 7-25 for more information.</td>
</tr>
<tr>
<td>Update State</td>
<td>Updates the door state displayed in the hardware tree.</td>
</tr>
</tbody>
</table>
Door Modes and Commands

### Set Door Mode Lock

Overrides the current door mode and locks the mechanism. The door mode remains set to Lock until you do one of the following:

- Select the command **Reset Door Mode** to return the door to the configured mode (such as the default mode or scheduled mode).
- Select a different **Set Door Mode** command.
- Reset the Gateway using the **Reset Gateway** command. You can also reboot the Gateway.
- Successfully execute the **Reload Gateway Configuration** command.
- Invoke the **Apply Configuration Changes** command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies).

**Note**  
Badge access is still allowed, or you can manually grant access with the **Grant Access** command.

### Set Door Mode Open

Overrides the door mode and unlocks the mechanism. The door mode remains set to Unlock until you do one of the following:

Overrides the current door mode and locks the mechanism. The door mode remains set to Lock until you do one of the following:

- Select the command **Reset Door Mode** to return the door to the configured mode (such as the default mode or scheduled mode).
- Select a different **Set Door Mode** command.
- Reset the Gateway using the **Reset Gateway** command. You can also reboot the Gateway.
- Successfully execute the **Reload Gateway Configuration** command.
- Invoke the **Apply Configuration Changes** command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies).

**Note**  
Badge access is still allowed, or you can manually grant access with the **Grant Access** command.

---

**Table 6-6  Door Commands in Locations View (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Door Mode Lock</td>
<td>Overrides the current door mode and locks the mechanism. The door mode remains set to Lock until you do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select the command <strong>Reset Door Mode</strong> to return the door to the configured mode (such as the default mode or scheduled mode).</td>
</tr>
<tr>
<td></td>
<td>• Select a different <strong>Set Door Mode</strong> command.</td>
</tr>
<tr>
<td></td>
<td>• Reset the Gateway using the <strong>Reset Gateway</strong> command. You can also reboot the Gateway.</td>
</tr>
<tr>
<td></td>
<td>• Successfully execute the <strong>Reload Gateway Configuration</strong> command.</td>
</tr>
<tr>
<td></td>
<td>• Invoke the <strong>Apply Configuration Changes</strong> command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Badge access is still allowed, or you can manually grant access with the <strong>Grant Access</strong> command.</td>
</tr>
<tr>
<td>Set Door Mode Open</td>
<td>Overrides the door mode and unlocks the mechanism. The door mode remains set to Unlock until you do one of the following:</td>
</tr>
<tr>
<td></td>
<td>Overrides the current door mode and locks the mechanism. The door mode remains set to Lock until you do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Select the command <strong>Reset Door Mode</strong> to return the door to the configured mode (such as the default mode or scheduled mode).</td>
</tr>
<tr>
<td></td>
<td>• Select a different <strong>Set Door Mode</strong> command.</td>
</tr>
<tr>
<td></td>
<td>• Reset the Gateway using the <strong>Reset Gateway</strong> command. You can also reboot the Gateway.</td>
</tr>
<tr>
<td></td>
<td>• Successfully execute the <strong>Reload Gateway Configuration</strong> command.</td>
</tr>
<tr>
<td></td>
<td>• Invoke the <strong>Apply Configuration Changes</strong> command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Badge access is still allowed, or you can manually grant access with the <strong>Grant Access</strong> command.</td>
</tr>
</tbody>
</table>
### Chapter 6 Configuring Doors

**Door Modes and Commands**

If a door includes a deadbolt device, this command overrides the door mode and applies the deadbolt. The deadbolt remains in place until you do one of the following:

- Overrides the current door mode and locks the mechanism. The door mode remains set to Lock until you do one of the following:
  - Select the command **Reset Door Mode** to return the door to the configured mode (such as the default mode or scheduled mode).
  - Select a different **Set Door Mode** command.
  - Reset the Gateway using the **Reset Gateway** command. You can also reboot the Gateway.
  - Successfully execute the **Reload Gateway Configuration** command.
  - Successfully execute the **Apply Configuration Changes** command (if no configuration changes were made, then no changes are sent to the Gateway. The previous door mode still applies).

**Note** Badge access is still allowed, or you can manually grant access with the **Grant Access** command.

**Table 6-6 Door Commands in Locations View (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Door Mode Secure</td>
<td>If a door includes a deadbolt device, this command overrides the door mode</td>
</tr>
<tr>
<td></td>
<td>and applies the deadbolt. The deadbolt remains in place until you do one of</td>
</tr>
<tr>
<td></td>
<td>the following:</td>
</tr>
<tr>
<td></td>
<td>- Overrides the current door mode and locks the mechanism. The door mode</td>
</tr>
<tr>
<td></td>
<td>remains set to Lock until you do one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Select the command <strong>Reset Door Mode</strong> to return the door to the</td>
</tr>
<tr>
<td></td>
<td>configured mode (such as the default mode or scheduled mode).</td>
</tr>
<tr>
<td></td>
<td>- Select a different <strong>Set Door Mode</strong> command.</td>
</tr>
<tr>
<td></td>
<td>- Reset the Gateway using the <strong>Reset Gateway</strong> command. You can also</td>
</tr>
<tr>
<td></td>
<td>reboot the Gateway.</td>
</tr>
<tr>
<td></td>
<td>- Successfully execute the <strong>Reload Gateway Configuration</strong> command.</td>
</tr>
<tr>
<td></td>
<td>- Successfully execute the <strong>Apply Configuration Changes</strong> command.</td>
</tr>
<tr>
<td></td>
<td>(if no configuration changes were made, then no changes are sent to the</td>
</tr>
<tr>
<td></td>
<td>Gateway. The previous door mode still applies).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Badge access is still allowed, or you can manually grant access</td>
</tr>
<tr>
<td></td>
<td>with the <strong>Grant Access</strong> command.</td>
</tr>
<tr>
<td>Reset Door Mode</td>
<td>Resets the door to the configured default mode.</td>
</tr>
<tr>
<td>Set Admin Down</td>
<td>Places the door in the Down state.</td>
</tr>
<tr>
<td>Set Admin Up</td>
<td>Places the door in the Up state.</td>
</tr>
<tr>
<td>Activate Access Levels</td>
<td>Manually activates the access levels for one or more doors. Use this command</td>
</tr>
<tr>
<td></td>
<td>if the access levels were deactivated.</td>
</tr>
<tr>
<td>Deactivate Access Levels</td>
<td>Manually deactivates all access levels for one or more doors. All access</td>
</tr>
<tr>
<td></td>
<td>is denied.                     Activate/deactivate access levels for multiple</td>
</tr>
<tr>
<td></td>
<td>doors:</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Locations &amp; Doors</strong> from the Doors menu, right click a</td>
</tr>
<tr>
<td></td>
<td>location and select <strong>Deactivate Access Levels</strong>. All doors in that</td>
</tr>
<tr>
<td></td>
<td>location are affected.</td>
</tr>
<tr>
<td></td>
<td>Activate/deactivate access levels for a single door:</td>
</tr>
<tr>
<td></td>
<td>- Right-click a door icon in the <strong>Locations &amp; Doors</strong> module and select</td>
</tr>
<tr>
<td></td>
<td>the command.</td>
</tr>
<tr>
<td></td>
<td>- In the <strong>Hardware</strong> module, expand the Logical Driver device tree,</td>
</tr>
<tr>
<td></td>
<td>right-click a door and select the command.</td>
</tr>
<tr>
<td></td>
<td>To reactive the access levels, select <strong>Activate Access Levels</strong>.</td>
</tr>
</tbody>
</table>

---
CHAPTER 7

Configuring Door and Device Templates

This chapter describes how to create and modify door and device templates. Device templates define common settings for device types, such as Gateways, readers and locks. Door templates define common settings for door configurations, including the devices that are attached to the door.

See Chapter 5, “Understanding Door Configuration” for more information.

Contents

- Creating Custom Gateway Configurations and Templates, page 7-2
- Configuring Door Templates, page 7-7
- Configuring Device Templates, page 7-14
- Configuring Credential Templates, page 7-17
- Configuring Reader LED Profiles, page 7-21
- Duplicating Templates, page 7-23
- Door Configuration Properties, page 7-25
- Device Configuration Properties, page 7-27
Creating Custom Gateway Configurations and Templates

Door configurations are sets of door device hardware assigned to a Gateway module. To create a door, a Gateway configuration must be created that defines the modules and devices attached to the Gateway. Gateway templates allow you to quickly populate that Gateway configuration.

To view the existing templates, select Gateway Templates from the Doors menu (in the Templates sub-menu).

Figure 7-1 shows the main window. The default Gateway templates cannot be changed. Only user-created templates can be modified.

**Figure 7-1** Gateway Templates Main Window
Procedure
Complete the following instructions to create a custom Gateway configuration, and then save it as a
template. You can also clone the configuration for use with another Gateway.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><img src="image1" alt="Display" /></td>
</tr>
<tr>
<td>Open the Hardware module in the Device view.</td>
<td><img src="image2" alt="Display" /></td>
</tr>
<tr>
<td>a. Select <strong>Hardware</strong> from the <strong>Doors</strong> menu.</td>
<td><img src="image3" alt="Display" /></td>
</tr>
<tr>
<td>b. Select <strong>Device</strong> from the <strong>View</strong> menu.</td>
<td><img src="image4" alt="Display" /></td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td><img src="image5" alt="Display" /></td>
</tr>
<tr>
<td>See also Viewing Doors and Devices in the Hardware View, page 5-3.</td>
<td><img src="image6" alt="Display" /></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><img src="image7" alt="Display" /></td>
</tr>
<tr>
<td>Add a Gateway module.</td>
<td><img src="image8" alt="Display" /></td>
</tr>
<tr>
<td>a. Right-click the <strong>Access GW Driver</strong>.</td>
<td><img src="image9" alt="Display" /></td>
</tr>
<tr>
<td>b. Select <strong>New Gateway Controller</strong>.</td>
<td><img src="image10" alt="Display" /></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><img src="image11" alt="Display" /></td>
</tr>
<tr>
<td>Select <strong>No</strong> to configure the Gateway without using a template.</td>
<td><img src="image12" alt="Display" /></td>
</tr>
<tr>
<td>Click <strong>Next</strong> to continue.</td>
<td><img src="image13" alt="Display" /></td>
</tr>
</tbody>
</table>
To do this

**Step 4**
Enter the basic Gateway properties.

a. **Name**: enter a descriptive name to identify the Gateway module.

b. **Serial Number**: enter the serial number. See Locating Serial Numbers, page 5-36.

c. **Location**: the assigned location of the module. See Creating the Location Map, page 5-6.

d. **Time Zone**: select the time zone for your system.

e. **Daylight Savings**: select True if Daylight Savings time is observed.

f. Click **Next** to add additional expansion modules.

or

Click **Finish** to create the Gateway controller (the default module) without adding additional modules.

**Step 5**
(Optional) Specify the expansion modules that are attached to the Gateway.

**Note** This step is only required if expansion modules are installed. If additional modules are not installed, click **Finish**.

**Note** The default module is the Gateway.

a. **Name**: enter a descriptive name to identify the Gateway module.

b. **Serial Number**: enter the serial number. See Locating Serial Numbers, page 5-36.

c. **Module Type**: select Reader, Input, or Output.

d. **Reader Connection Mode**: (Reader modules only) select if the device supports one or two reader connections.

e. Click **Add**. The expansion module is added to the list.

f. Repeat these steps for each additional module.

Click **Finish** to save the changes and close the window.

**Tip** To modify the module list, select a module and click **Edit** or **Remove**.
Step 6

(Optional) Add devices to the Gateway or expansion module interfaces.

**Note** Devices are usually added when configuring a door. See Chapter 6, “Configuring Doors”.

- Expand the hardware tree to view the Gateway or expansion module interfaces.
- Right-click an interface and select the device for the interface. For example: New REX.
- In the device window, select **Properties** and enter the device settings.
  - Select a **Template name** to populate the fields.
  - To override the template settings, deselect the **Default** checkbox next to each field.
  - To restore the default template setting, re-select the **Default** checkbox.
- Click **Save and Close**.
- Repeat these steps for each device connected to the Gateway.

Step 7

Apply the configuration changes to download the new settings to the devices.

- To update all Gateways: right-click the Access GW Driver and select **Apply Configuration Changes**.
- To update a Single Gateway: right-click the 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. For more information, see Applying Configuration Changes, page 6-17.
Creating Custom Gateway Configurations and Templates

Chapter 7 Configuring Door and Device Templates

Step 8  
(Optional) Create a Gateway template from the new configuration.

- Right-click on the Gateway Controller and select **Save As Gateway Template**. Enter a name for the template and click **OK**. The new template is displayed in the main Gateway templates window (see Figure 7-1)
- Select **Clone Gateway** to create an exact copy of a Gateway configuration for a single Gateway. See **Cloning a Gateway Configuration**, page 6-27.

Step 9  
(Optional) Add the door configuration that use the ports on the Gateway. See **Configuring Doors**, page 6-2.
Chapter 7 Configuring Door and Device Templates

Configuring Door Templates

Use door templates to create sets of hardware that can be applied to multiple doors. For example, you can create a template that includes a door swing for use with ADA-enabled doors, or a dead bolt for doors that require extra security. See Chapter 5, “Understanding Door Configuration” for more information.

Figure 7-2 Door Templates Main Window

Note

The default templates are read-only. Only user-created door templates can be modified.

To create or modify a door template, do the following:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td>Select Door Templates from the Doors menu, in the Templates sub-menu.</td>
<td>Select Door Templates from the Templates sub-menu.</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring Door and Device Templates

Configuring Door Templates

Step 2
Click Add, or select an existing template and click Edit or Duplicate.

- You can also right-click an entry and select Add, Edit, or Delete.
- To duplicate an existing template:
  - Select the template and click the Duplicate button in the upper right.
  - Enter a New Name for the template and click OK.
  - In the main window, select the duplicate template name and click Edit.
  - Revise the template settings as described in the following steps.

Step 3
Click the General tab and enter the Name and Description for the template.

Step 4
Select the devices for in the door template:

a. Select the Devices tab.

b. Click Add to add a new device or select an existing device from the list and click Edit.

c. Select the Device Type. For example: Lock, Reader, etc.

d. Select the Template. Only the templates for the device type are displayed. For example, if the device type is Reader, then only reader templates are displayed. See Configuring Device Templates, page 7-14 for instructions to create and modify the available templates.

e. Repeat these steps to add additional devices, if necessary.

f. Click Next to continue.
Step 5

Define the door lock properties.

a. Select the Properties tab.

b. **Re lock interval time (sec):** the number of seconds to keep the door open after an access request is granted (grant access).

c. **Door held open time (sec):** the number of seconds before the DoorHelpOpen alarm is generated.

d. **Door lock on close:**
   - The default is Yes. The door will always lock when closed, overriding the Re lock interval time (even if a second request was entered while the door was open).
   
   - Select No to keep the door unlocked for the duration of the Re lock interval time, even if it is closed. The relock time is based on the most recent access request for the door.

e. **Deadbolt engage delay (sec):** the delay (in seconds) after a door closes until the deadbolt is applied.

Usage Notes

By default, when a door access request is granted, the door remains unlocked until the Re lock interval time elapses, or until the door is closed again, whichever comes first. In some situations, you may want to keep the door unlocked for the entire interval time, even when it is closed again. For example:

1. When a door is unlocked by user “A” the Re lock interval time is triggered. The door will automatically relock when the relock time is met, or when the door is open and then closed again.

2. Before user “A” approaches the door and opens it, a handicapped person, user “B”, also presents a badge. Access is granted and the Re lock interval time is extended to reflect this latest grant access request.

3. In the meantime, however, user “A” opens the door and closes the door behind him (while user “B” is several feet away from the door). The door is automatically relocked since Door lock on close is set to Yes by default.

4. To keep the door unlocked until the Re lock interval time is elapsed for the most recent request, set Door lock on close to No.
### Configuring Door Templates

**Step 6** Define the door mode and schedule:

a. Select the **Properties** tab.

b. **Default mode**: select the default door mode. The door remains in this mode at all times except when a schedule is defined.
   - **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.

See [Door Modes, page 6-39](#) for more information.

c. **Door enable schedule**: (optional) select a door schedule. If you select **None**, then the door will remain in the **Default** mode at all times. If you select a schedule, the schedule will override the default mode for the times and days defined in the schedule. See [Using the Schedule Manager, page 9-7](#) to add or modify the available door schedules.

d. **Scheduled door mode**: select the door mode when the door scheduled is applied.

   For example, if the Default mode is Lock, and the scheduled door mode is Close, then the door will be locked at all times except during the hours and days defined by the schedule selected in **Door enable schedule**.

e. **First Unlock**: select **First Unlock** to activate the door schedule only on 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. This is useful in situations such as snow days to ensure the door is not opened until a badge holder is physically present.

**Tip** See [Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 5-25](#) for more information.
To do this | Use this display
--- | ---
**Step 7** Enter the additional door **Properties:** | ![Image](image.jpg)
- **Relock interval time (sec):** see Step 5.
- **Door held open time (sec):** see Step 5.
- **Door lock on close:** see Step 5.
- **Deadbolt engage delay (sec):** see Step 5.
- **Scheduled Door Mode:** see Step 6.
- **Door enable schedule:** see Step 6.
- **First Unlock:** see Step 6.
- **Default Mode:** see Step 6.
- **If badge not in gateway:** the action taken by the Gateway if the badge is not in the Gateway database.
- **Access decision on timeout:** the action taken by the Gateway if there is no response within *Server access timeout.*
- **If server unreachable:** the action to be taken by gateway in case it cannot reach Cisco PAM.
- **Server access timeout (sec):** the number of seconds before an action is taken based on *Access decision on timeout.*
- **ADA timespec multiplier:** the multiplier used on *Relock interval time* if an ADA access occurs.
- **Door swing activation delay (sec):** the number of seconds before the door swing is activated. This setting allows time for the door lock or other devices to activate before the mechanical door swing activates.
- **Door swing usage:**
  - **Always operate:** the door swing activates for all access requests.
  - **Operate for ADA only:** the door swing operates only for requests from an ADA device.
  - **Do not operate:** the door swing does not operate.
<table>
<thead>
<tr>
<th>Step 8</th>
<th>Configuring Door Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To do this</strong></td>
<td><strong>Usage Profiles</strong> used by the reader device(s). These profiles define what LED or buzzer action occurs under the following events:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Grant access</strong>: the LED display when normal access is granted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Grant access ADA</strong>: the LED display when access is granted for an ADA enabled badge.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deny access</strong>: the LED display when access is denied.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Grant facility code</strong>: the LED display when access is granted based on a Facility Code.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mode open</strong>: the LED display when the door mode is <em>Open</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mode close</strong>: the LED display when the door mode is <em>Close</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mode lock</strong>: the LED display when the door mode is <em>Lock</em>.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>See Configuring Reader LED and Buzzer Profiles, page 7-22 for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Configuring Door Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To do this</strong></td>
<td><strong>Facility Code Info</strong>:</td>
</tr>
<tr>
<td></td>
<td>Click <em>Add</em> to add a credential template and facility code.</td>
</tr>
<tr>
<td></td>
<td>Each card format has a facility code associated with the card. All the card formats used with the door must be specified. The Gateway can also be configured to use facility codes during <em>Server Unreachable</em> and <em>Server Access Timeout</em> if necessary.</td>
</tr>
<tr>
<td>Step</td>
<td>To do this</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>10</td>
<td>Enter the Duress Specifications. Click Add to add an alarm type and code.</td>
</tr>
<tr>
<td>11</td>
<td>Click Save and Close to save the template and close the window.</td>
</tr>
</tbody>
</table>
Configuring Device Templates

Device templates are pre-defined configurations for the device types using in door configurations. Device templates are used to create door templates, or they can be applied directly to a Gateway interface.

This section includes instructions to create device templates.

Note
Most settings in the default templates are read-only. Only user-created door templates can be modified.

Figure 7-3  Device Templates Main Window

For more information, see Chapter 5, “Understanding Door Configuration” and Chapter 6, “Configuring Doors”.

Cisco Physical Access Manager User Guide
Creating a Device Template

Use the Device Template Wizard to create a new device template.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><img src="image1.png" alt="Device Template Wizard" /></td>
</tr>
<tr>
<td>Select Device Templates from the Doors menu, in the Templates sub-menu.</td>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select Add..., and then select Device Template Wizard.</td>
</tr>
<tr>
<td>You can also do the following:</td>
<td>Select Add..., and then select Device Template Wizard.</td>
</tr>
<tr>
<td>- You can also select an existing device from the list and click Edit or Duplicate. To duplicate an existing template:</td>
<td>- You can also select an existing device from the list and click Edit or Duplicate. To duplicate an existing template:</td>
</tr>
<tr>
<td></td>
<td>- Select the template and click the Duplicate button in the upper right.</td>
</tr>
<tr>
<td></td>
<td>- Enter a New Name for the template and click OK.</td>
</tr>
<tr>
<td></td>
<td>- In the main window, select the duplicate template name and click Edit.</td>
</tr>
<tr>
<td></td>
<td>- Revise the template settings as described in the following steps.</td>
</tr>
</tbody>
</table>
| - Right-click on a template name to access the Edit and Delete functions. | - Right-click on a template name to access the Edit and Delete functions. | - Right-click on a template name to access the Edit and Delete functions. | - Right-click on a template name to access the Edit and Delete functions.
### Configuring Device Templates

**Step 3**  
Select the **Device Template Type**, and then click **Next**.

**Use this display**

- **Create New Device Template**
  - Choose Device Template
  - Device template types: [Deadbolt Interface, Door Status Template, Ductless Door Sensor Template, Fire Sensor Template, Generic Input Template, Generic Output Template, Glass-break Sensor Template, Lock Template, Power Fail Template, REX Template, Reader Template, Sensor Template, Tamper Template]
  - Description:
  - Output Device:

**Step 4**  
Enter the device settings. This example is for a REX device. The fields available vary depending on the device type.

- **a.** Enter the template **Name**.
- **b.** Enter the device settings. See **Device Configuration Properties, page 7-27** for detailed information about the options for each device type. The settings are different for each type of device.
- **c.** Click **Finish** to save the template and close the window.
Chapter 7 Configuring Door and Device Templates

Configuring Credential Templates

Create templates define the settings for credential devices, such as Wiegand readers and keypads. Credential templates are applied to reader devices or to door templates.

- Overview, page 7-17
- Credential Templates Settings Summary, page 7-18
- Creating a Credential Template, page 7-19

Overview

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 Credential Templates Settings Summary, page 7-18 for a configuration overview.

Existing templates cannot be modified. See Creating a Credential Template, page 7-19 for instructions to create a new template.

Figure 7-4 Credential Templates Main Window
Credential Templates Settings Summary

Cisco PAM supports credential templates for the following:

- **Wiegand Keypad**
- **Wiegand**
- **Keypad**

The template is based on the type of Reader.

**Note**

Credential templates with the same length in bits for the Primary data cannot be associated with the same reader device; the templates must be associated with different devices. However, credential templates with different length in bits for the Primary data can be associated with the same reader device.

**Wiegand Keypad**

The keypad data is transported using the Wiegand protocol (when the user enters a pin on the keypad, the data is transported to the reader in the Wiegand frame). The credential template has two decoding configurations.

- The first decoding configuration (Primary) specifies how to extract the pins data entered by the user.
- Once the pins data is extracted, the second decoding configuration (Secondary) specifies how to extract each pin, by specifying the total length, length of each pin, parity etc.

For example, the `26BitWiegandKeypadCT`.

**Wiegand**

Card data is transported over Wiegand protocol. When the user swipes or flashes the badge, the card data is transported to the reader in the Wiegand frame. Only the first decoding configuration (Primary) is required to specify the extraction of card data fields such as Card ID, Facility, Site, and Other. Parity and sentinel is used to validate the data.

For example, the `26BitWiegandCT`.

**Keypad**

The keys pressed by a user are directly transported to the reader, so only the Primary decoding configuration is required.

For example, the `KeyPad_BCD4`.
Creating a Credential Template

Complete the following instructions to create, edit, or duplicate a credential template.

**Step 1** Select **Credential Templates** from the Doors menu, in the Templates sub-menu.

**Step 2** Click **Add** or select an existing template from the list and click **Edit**.

- You can also select an existing device from the list and click **Edit** or **Duplicate**. To duplicate an existing template:
  - Select the template and click the **Duplicate** button in the upper right.
  - Enter a **New Name** for the template and click **OK**.
  - In the main window, select the duplicate template name and click **Edit**.
  - Revise the template settings as described in the following steps.

- You can also or right-click on a template name to access the **Add**, **Edit** and **Delete** functions.

**Step 3** Select the General tab, enter the **Name** and **Description** of the template.
<table>
<thead>
<tr>
<th>Step 4</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the <strong>Primary Data</strong> and <strong>Secondary Data</strong> settings for the template.</td>
<td><img src="image" alt="Add Credential Template" /></td>
<td></td>
</tr>
<tr>
<td>See <strong>Credential Templates Settings Summary</strong>, page 7-18 for more information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Credential templates with the same length in bits for the Primary data cannot be associated with the same reader device; the templates must be associated with different devices. However, credential templates with different length in bits for the Primary data can be associated with the same reader device.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click <strong>Save and Close</strong> to save the template and close the window.</td>
<td><img src="image" alt="Save and Close" /></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Reader LED Profiles

**Reader LED Profiles** define the LED lights and buzzer on the reader interface of a Gateway or Reader module. The profiles are used to configure the Usage Profiles in door templates. The profiles can also be applied to reader interfaces in the Hardware module.

*Figure 7-5 Reader UI Profile Main Window*
### Configuring Reader LED and Buzzer Profiles

The reader interface provides up to three output lines to control connections for LEDs or a buzzer. A typical reader includes connections for the red LED, green LED and a buzzer. Most readers use only one or two of these.

Complete the following instructions to configure LED profiles.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><img src="https://example.com/image1.png" alt="Image" /></td>
</tr>
<tr>
<td>Select <strong>Reader LED Profiles</strong> from the Doors menu, in the Templates sub-menu.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><img src="https://example.com/image2.png" alt="Image" /></td>
</tr>
<tr>
<td>Create or edit the profile:</td>
<td></td>
</tr>
<tr>
<td>a. Click <strong>Add</strong>, or select an existing profile and click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>You can also right-click on an item to access the <strong>Add</strong>, <strong>Edit</strong> and <strong>Delete</strong> functions.</td>
</tr>
<tr>
<td>b. Enter the profile <strong>Name</strong>.</td>
<td></td>
</tr>
<tr>
<td>c. Enter the profile settings:</td>
<td></td>
</tr>
<tr>
<td>- <strong>Command</strong>: defines the state of the output when the profile is invoked (<strong>Output On</strong> or <strong>Output Off</strong>).</td>
<td></td>
</tr>
<tr>
<td>- <strong>Duration</strong>: specifies how long the output is turned on and off.</td>
<td></td>
</tr>
<tr>
<td>- <strong>Repeat</strong>: specifies the number of times the output is turned on and off.</td>
<td></td>
</tr>
<tr>
<td>- <strong>On time (ms)</strong> and <strong>Off time (ms)</strong>: specifies how long the output is ON or OFF, in milliseconds.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><img src="https://example.com/image3.png" alt="Image" /></td>
</tr>
<tr>
<td>Click <strong>Save and Close</strong> to save the profile and close the window.</td>
<td></td>
</tr>
</tbody>
</table>

Duplicating Templates

- Duplicating Door, Device, and Credential Templates, page 7-23
- Duplicating Gateway Templates, page 7-24

Duplicating Door, Device, and Credential Templates

In situations where you need a template that is similar to an existing template, use the Duplicate feature to create an exact copy of the template, and then edit the new template settings as necessary.

To create exact duplicates of door, device, and credential templates, do the following:

**Step 1** Select Templates from the Doors window and select a template type: Door, Device, or Credential.

**Step 2** Highlight an existing template entry.

**Step 3** Click the Duplicate button in the upper right of the window, as shown in Figure 7-6.

**Figure 7-6 Duplicates Button in Door Template Window**

**Step 4** Enter a New Name for the template and click OK, as shown in Figure 7-7.

**Figure 7-7 Duplicates Name**

**Step 5** In the main window, select the new template name and click Edit.

**Step 6** Revise the template settings as described in the appropriate configuration section:

- Configuring Door Templates, page 7-7
- Configuring Device Templates, page 7-14
Duplicating Gateway Templates

- To create a template from a Gateway configuration, see Creating Custom Gateway Configurations and Templates, page 7-2.

- To create a clone of a Gateway configuration for one-time use, see Cloning a Gateway Configuration, page 6-27. A Gateway clone is an independent copy, and is used to configure one other Gateway module.
Door Configuration Properties

The following properties are configured for a door template and configuration.
See Configuring Door Templates for more information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relock interval time (sec)</td>
<td>the number of seconds to keep the door open after an access request is granted (grant access).</td>
</tr>
<tr>
<td>Door held open time (sec)</td>
<td>The number of seconds before DoorHelpOpen alarm is generated.</td>
</tr>
<tr>
<td>Door lock on close</td>
<td>The default is Yes. The door will always lock when closed, overriding the Relock interval time (even if a second request was entered while the door was open). Select No to keep the door unlocked for the duration of the Relock interval time, even if it is closed. The relock time is based on the most recent access request for the door.</td>
</tr>
<tr>
<td>Deadbolt engage delay (sec)</td>
<td>The amount of time to wait (in seconds) after the door closes to engage the deadbolt.</td>
</tr>
<tr>
<td>Scheduled door mode</td>
<td>The schedule set when a door scheduled is applied in Door enable schedule. For example if the Default mode is Lock, and the scheduled door mode is Close, then the door will be locked at all times except during the hours and days defined by the schedule selected in Door enable schedule. See Understanding Door Modes, Door Schedules, and the First Unlock Feature.</td>
</tr>
<tr>
<td>Door enable schedule</td>
<td>The schedule to be used by Door. If you select None, then the door will remain in the Default mode at all times and days. If you select a schedule, the schedule overrides the default mode for the times and days defined in the schedule. See Using the Schedule Manager, page 9-7 to add or modify the available door schedules. See also Understanding Door Modes, Door Schedules, and the First Unlock Feature.</td>
</tr>
<tr>
<td>First unlock</td>
<td>Activates the door schedule on the first successful badge swipe (during the scheduled time span). If the door is not physically accessed, then the door remains locked. Also known as “Snow day”. The door remains in default mode until a badge is used to access the door, even after the beginning time for the schedule. This is useful in situations such as snow days to ensure the door is not opened until a badge holder attempts to enter the door.</td>
</tr>
</tbody>
</table>

Note: See Understanding Door Modes, Door Schedules, and the First Unlock Feature for more information.
### Door Configuration Properties

#### Default mode
The door mode used in non-scheduled times. The door remains in this mode at all times except when a schedule is defined.
- **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.

See Understanding Door Modes, Door Schedules, and the First Unlock Feature for more information.

#### If badge not in gateway
The action taken by the Gateway if the badge is not in the Gateway database.

#### Access decision on timeout
The action taken by the Gateway if there is no response within Server access timeout.

#### If server unreachable
The action to be taken by gateway in case it cannot reach Cisco PAM.

#### Server access timeout (sec)
The number of seconds before an action is taken based on Access decision on timeout.

#### ADA timespec multiplier
The multiplier used on Relock interval time if an ADA access occurs.

#### Door swing activation delay (sec)
The number of seconds before the door swing is activated. This setting allows time for the door lock or other devices to activate before the mechanical door swing activates.

#### Door swing usage
Select one of the following:
- **Always operate**: the door swing activates for all access requests.
- **Operate for ADA only**: the door swing operates only for requests from an ADA device.
- **Do not operate**: the door swing does not operate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default mode</td>
<td>The door mode used in non-scheduled times. The door remains in this mode at all times except when a schedule is defined.</td>
</tr>
<tr>
<td>If badge not in gateway</td>
<td>The action taken by the Gateway if the badge is not in the Gateway database.</td>
</tr>
<tr>
<td>Access decision on timeout</td>
<td>The action taken by the Gateway if there is no response within Server access timeout.</td>
</tr>
<tr>
<td>If server unreachable</td>
<td>The action to be taken by gateway in case it cannot reach Cisco PAM.</td>
</tr>
<tr>
<td>Server access timeout (sec)</td>
<td>The number of seconds before an action is taken based on Access decision on timeout.</td>
</tr>
<tr>
<td>ADA timespec multiplier</td>
<td>The multiplier used on Relock interval time if an ADA access occurs.</td>
</tr>
<tr>
<td>Door swing activation delay</td>
<td>The number of seconds before the door swing is activated. This setting allows time for the door lock or other devices to activate before the mechanical door swing activates.</td>
</tr>
<tr>
<td>Door swing usage</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Always operate</strong>: the door swing activates for all access requests.</td>
</tr>
<tr>
<td></td>
<td><strong>Operate for ADA only</strong>: the door swing operates only for requests from an ADA device.</td>
</tr>
<tr>
<td></td>
<td><strong>Do not operate</strong>: the door swing does not operate.</td>
</tr>
</tbody>
</table>
Device Configuration Properties

Table 7-2 describes device settings for common device types.

Note

Normally open (NO) contacts connect the circuit when the relay is activated; the circuit is disconnected when the relay is inactive.

Normally closed (NC) contacts disconnect the circuit when the relay is activated; the circuit is connected when the relay is inactive.

Table 7-2  Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deadbolt</td>
<td>• <strong>Name</strong>: The template name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Model</strong>: The device model.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Vendor</strong>: The device vendor or manufacturer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong>: A text description of the device.</td>
</tr>
<tr>
<td>Door Swing</td>
<td>• <strong>Name</strong>: The template name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Model</strong>: The device model.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Vendor</strong>: The device vendor or manufacturer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong>: A text description of the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Trigger Time (sec)</strong>: The number of seconds that power is applied to operate the door swing.</td>
</tr>
<tr>
<td>Door Sensor</td>
<td>• <strong>Sensor input</strong>: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Open</strong>: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Closed</strong>: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supervised</strong>: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device state</strong>: The default state of the device.</td>
</tr>
<tr>
<td>Duress Sensor</td>
<td>• <strong>Sensor input</strong>: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Open</strong>: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Closed</strong>: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supervised</strong>: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sensor state</strong>: The default state of the device.</td>
</tr>
<tr>
<td>Fire Sensor</td>
<td>• <strong>Sensor input</strong>: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Open</strong>: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Closed</strong>: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supervised</strong>: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device state</strong>: The default state of the device.</td>
</tr>
</tbody>
</table>
### Table 7-2  Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Generic Input Device</strong></td>
<td>• <strong>Normal state</strong>: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Open</strong>: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Closed</strong>: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supervised</strong>: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device state</strong>: The default state of the device.</td>
</tr>
<tr>
<td><strong>Generic Output Device</strong></td>
<td>• <strong>Name</strong>: The template name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Model</strong>: The device model.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Vendor</strong>: The device vendor or manufacturer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong>: A text description of the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activation Time (ms)</strong>: When the command <code>Timed Activate Relay</code> is invoked,</td>
</tr>
<tr>
<td></td>
<td>this property defines the number of milliseconds the generic output is activated.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In Cisco PAM Release 1.1.0 and higher, generic output and lock devices must use the physical wire connections to the Gateway or expansion module to define if the device is <em>normally open</em> or <em>normally closed</em>. In Cisco PAM Release 1.0.3 or earlier, this setting could also be made in software. If you are upgrading from Cisco PAM Release 1.0.3 or earlier, verify that devices are correctly wired to the module as <em>normally open</em> or <em>normally closed</em>. See <em>Cisco Physical Access Gateway User Guide</em> for more information.</td>
</tr>
<tr>
<td><strong>Glass-Break</strong></td>
<td>• <strong>Sensor input</strong>: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Open</strong>: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– <strong>Normally Closed</strong>: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supervised</strong>: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sensor state</strong>: The default state of the device.</td>
</tr>
<tr>
<td><strong>Lock</strong></td>
<td>• <strong>Name</strong>: The template name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Model</strong>: The device model.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Vendor</strong>: The device vendor or manufacturer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong>: A text description of the device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In Cisco PAM Release 1.1.0 and higher, generic output and lock devices must use the physical wire connections to the Gateway or expansion module to define if the device is <em>normally open</em> or <em>normally closed</em>. In Cisco PAM Release 1.0.3 or earlier, this setting could also be made in software. If you are upgrading from Cisco PAM Release 1.0.3 or earlier, verify that devices are correctly wired to the module as <em>normally open</em> or <em>normally closed</em>. See <em>Cisco Physical Access Gateway User Guide</em> for more information.</td>
</tr>
</tbody>
</table>
### Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motion Sensor</td>
<td>• Name: The template name.</td>
</tr>
<tr>
<td></td>
<td>• Model: The device model.</td>
</tr>
<tr>
<td></td>
<td>• Vendor: The device vendor or manufacturer.</td>
</tr>
<tr>
<td></td>
<td>• Description: A text description of the device.</td>
</tr>
<tr>
<td></td>
<td>• Normal state: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– Normally Open: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– Normally Closed: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• Supervised: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• Device state: The default state of the device.</td>
</tr>
</tbody>
</table>

| Power Fail | • Normal state: The type of device contact:     |
|            |   – Normally Open: the device is normally open. |
|            |   – Normally Closed: the device is normally closed.|
|            | • Supervised: Defines if the device is supervised or unsupervised. |
|            | • Device state: The default state of the device.|

<table>
<thead>
<tr>
<th>REX</th>
<th>Note</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Rex input: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Normally Open: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Normally Closed: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device state: The default state of the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Supervised: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Push button: Indicates a push button type of REX.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Push button type: Indicates the kind of push button REX.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ADA enabled: Indicates if ADA is enabled or not. If ADA is enabled, ADA timespec multiplier property is applied on the door when REX is activated.</td>
</tr>
</tbody>
</table>
### Device Configuration Properties

<table>
<thead>
<tr>
<th>Device</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader</td>
<td>• Reader type:</td>
</tr>
<tr>
<td></td>
<td>– Card Reader</td>
</tr>
<tr>
<td></td>
<td>– Card and Keypad Reader</td>
</tr>
<tr>
<td></td>
<td>– Keypad Reader</td>
</tr>
<tr>
<td></td>
<td>• Protocol: Only Wiegand is supported.</td>
</tr>
<tr>
<td></td>
<td>• Data format: Only Standard Wiegand is supported.</td>
</tr>
<tr>
<td></td>
<td>• Credential template: Set of credential templates to be used to validate the cards presented to this reader.</td>
</tr>
<tr>
<td></td>
<td>• Category: Entry or Exit reader.</td>
</tr>
<tr>
<td></td>
<td>• Reader connector: Type of connector Ten Wire/Five Wire</td>
</tr>
<tr>
<td></td>
<td>• Use hold pin: Flag specifying if the Hold control line is part of the Reader. Not all readers have or use the Hold control line.</td>
</tr>
<tr>
<td></td>
<td>• Credential order: If the reader is a Card and Keypad Reader this field specifies the credentials order.</td>
</tr>
<tr>
<td></td>
<td>• Maximum timeout (sec): If the reader includes a keypad, this field specifies the maximum time to wait for the user to enter the pins using the keypad.</td>
</tr>
<tr>
<td></td>
<td>• ADA enabled: Specifies if it is an ADA enabled reader. If ADA is enabled, the ADA timespec multiplier door property is used when a valid card with ADA flag set is presented to the reader.</td>
</tr>
<tr>
<td></td>
<td>• Number of duress keys: If the reader has a keypad, this field specifies the length of duress key. If the duress key or triggers as configured on the door is “89898”, then the value of this field is 5.</td>
</tr>
<tr>
<td></td>
<td>• Number of pin keys: If the reader has a keypad, this field specifies the length of the pin to expect.</td>
</tr>
<tr>
<td></td>
<td>• Keys buffered: Specifies if the pins entered are transferred in one frame (keys buffered) or in individual frames (keys not buffered). This is field is set based what is supported by the reader/keypad.</td>
</tr>
<tr>
<td>Tamper</td>
<td>• Tamper input: The type of device contact:</td>
</tr>
<tr>
<td></td>
<td>– Normally Open: the device is normally open.</td>
</tr>
<tr>
<td></td>
<td>– Normally Closed: the device is normally closed.</td>
</tr>
<tr>
<td></td>
<td>• Supervised: Defines if the device is supervised or unsupervised.</td>
</tr>
<tr>
<td></td>
<td>• Tamper state: The default state of the device.</td>
</tr>
</tbody>
</table>
CHAPTER 8

Configuring Personnel and Badges

This chapter describes how to create the personnel records and badges used to access doors in the Cisco Physical Access Control system.

Note
For instructions to synchronize Cisco PAM with personnel records from another database, see Chapter 12, “System Integration”.

Contents

- Configuring Personnel, page 8-2
- Downloading Credential Changes to the Gateway Modules, page 8-10
- Viewing Audit Records and Events for Personnel Records, page 8-11
- Editing Organization and Department Lists, page 8-13
- Importing Personnel Records Using a Comma Separated Value (CSV) File, page 8-15
- Configuring Badges, page 8-20
  - Configuring Badge Templates, page 8-20
  - Badge Properties, page 8-22
  - Using the Badge Designer, page 8-28
  - Printing Badges, page 8-35
- Setting Up Image and Signature Options for Personnel Records, page 8-44
Configuring Personnel

Use the Personnel module to manage personnel records. Personnel records contain information on the site's personnel, such as employees, contractors, and visitors. A personnel record may have associated credentials, such as badges or logins.

Tip

Personnel records are unique based on the ID number of the record. If a record is imported with the same ID number, then the current record is updated with the new data.

This section describes how to manage personnel, including adding an image, a badge, and an associated access level.

Step 1
Open the Personnel module from the Users menu, as shown in Figure 8-2.

Step 2
To add a personnel record, choose Add (Advanced)....

- To modify an existing record, select the entry and click Edit.
- To edit all records displayed in the list, click Group Edit.... See Using Group Edit, page 3-14 for more information.
- To disable a record, select the entry and choose Disable. This is equivalent to setting the Status to Inactive.

Figure 8-1 Personnel Module: Main Window

Step 3
Enter the information in the General tab, as shown in Figure 8-2. See Table 8-1 for field descriptions. The first name, last name, and SSN/FIN>ID fields are required.
Figure 8-2  General

![General Tab](image)

### Table 8-1 Personnel Module: General Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>(Optional) The person’s formal title. Select a value from the drop-down menu (such as Dr., Mr., or Ms.) or enter the text manually.</td>
</tr>
<tr>
<td>First name</td>
<td>(Required) The person's given name.</td>
</tr>
<tr>
<td>Middle name</td>
<td>(Optional) The person's middle name.</td>
</tr>
<tr>
<td>Last name</td>
<td>(Required) The person's surname (family name).</td>
</tr>
<tr>
<td>Suffix</td>
<td>(Optional) The suffix at the end of the person's name. Select a value from the drop-down menu (such as I, II, III, Jr., and Sr.) or enter the text manually.</td>
</tr>
<tr>
<td>Date of birth</td>
<td>(Optional) The person's birth date.</td>
</tr>
</tbody>
</table>
| SSN/ID#/FIN   | (Required) Select the type of ID number used from the drop-down menu, and enter the actual number in the field to the right.  
**Note** Personnel records are unique based on the ID number of the record. If a record is imported with the same ID number, then the current record is updated with the new data. |
| Comments      | (Optional) Any additional comments or notes about the personnel record.     |
| Site          | (Optional) The site associated with the personnel record.                   |
| Import...     | (Optional) Click Import... to add an image to the record (select a JPEG image from a local drive and click OK). |

**Step 4** (Optional) Add an image to the personnel record:

a. Click the Capture... button to open an image capture device interface.
   
   - If a picture has already been taken, click the Import... button and browse to the desired JPEG image for the person's picture and click the OK button and skip to step 8.

   - If the Capture... button is grayed out, enable the capture device in the properties section (see Enabling Image Capture Devices, page 8-44).
b. Use the built in tools to pan, tilt and zoom to the appropriate location. Once satisfied with the camera settings click the **Capture** button to take a picture. After clicking the **Capture** button a preview of the picture will be displayed.

c. Click the **Save** button to save the picture or the **Capture** button to take another picture. Once the **Save** button is selected the **Capture Image** wizard will open. Using the mouse move the highlighted box to the appropriate location. The area within the highlighted box will be saved within the personnel record.

d. Click **Next** to preview the finalized image. Click the **Finish** button to close the wizard and preview the image within the new personnel record.

**Step 5** (Optional) Add a signature to the personnel record. See [Enabling Signature Capture Devices](#) for more information.

**Step 6** Enter the **Occupational Information** for the personnel record, as shown in Figure 8-3. See Table 8-2 for field descriptions.

**Figure 8-3** Occupational Information

![Figure 8-3 Occupational Information](image)

**Table 8-2** Personnel Module: Occupational Information Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title in organization</td>
<td>The person’s title within the organization. For example, Director of Engineering.</td>
</tr>
<tr>
<td>Employee number</td>
<td>The employee number, if applicable. Generally, but not required to be, unique.</td>
</tr>
</tbody>
</table>
Table 8-2  Personnel Module: Occupational Information Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel Type</td>
<td>The type of employee. Options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Contractor</td>
</tr>
<tr>
<td></td>
<td>• Employee - Full Time</td>
</tr>
<tr>
<td></td>
<td>• Employee - Part Time</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td></td>
<td>• Visitor</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the employee. Options include the following:</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Inactive</td>
</tr>
<tr>
<td></td>
<td>• On Leave</td>
</tr>
<tr>
<td></td>
<td>• Retired</td>
</tr>
<tr>
<td></td>
<td>• Terminated</td>
</tr>
<tr>
<td>Organization</td>
<td>The organization name to which the person belongs. Select a pre-defined</td>
</tr>
<tr>
<td></td>
<td>value from the drop-down menu, or type a name in the field. To edit the</td>
</tr>
<tr>
<td></td>
<td>pre-defined options, see Editing Organization and Department Lists, page 8-13</td>
</tr>
<tr>
<td>Department</td>
<td>The department name within the organization to which the person belongs.</td>
</tr>
<tr>
<td></td>
<td>Select a pre-defined department name from the drop-down menu, or enter a</td>
</tr>
<tr>
<td></td>
<td>name in the field. To edit the pre-defined options, see Editing Organization</td>
</tr>
<tr>
<td></td>
<td>and Department Lists, page 8-13</td>
</tr>
<tr>
<td>Date of hire</td>
<td>The date the employee was hired.</td>
</tr>
</tbody>
</table>

Step 7 Enter the Contact Information for the personnel record, as shown in Figure 8-4. See Table 8-3 for field descriptions.
Configuring Personnel

Figure 8-4  Contact Information

Table 8-3  Personnel Module: Contact Information Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The physical and/or mailing address(es) of the person. Each record can contain up to three different addresses:</td>
</tr>
<tr>
<td></td>
<td>• Work</td>
</tr>
<tr>
<td></td>
<td>• Home</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>Phone numbers</td>
<td>The telephone number(s) for the person. Each record can contain up to five different phone numbers:</td>
</tr>
<tr>
<td></td>
<td>• Work</td>
</tr>
<tr>
<td></td>
<td>• Home</td>
</tr>
<tr>
<td></td>
<td>• Mobile</td>
</tr>
<tr>
<td></td>
<td>• Fax</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address(es) for the person. Each record can contain up to three different email addresses:</td>
</tr>
<tr>
<td></td>
<td>• Primary</td>
</tr>
<tr>
<td></td>
<td>• Secondary</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
</tbody>
</table>

Step 8  Add a badge to the personnel record.

a. Click the Badges tab
b. Click the Add... button to open the badge template window.

c. Select a template from the menu and click OK. To configure a badge without using a template, select None.

See Configuring Badge Templates, page 8-20 to create or modify the templates.

d. Enter the Card # and PIN (required) in the badge properties window, as shown in Figure 8-5.

e. Modify the other badge fields, if necessary, as described in Badge Properties, page 8-22.

f. Click Save and Close to save the badge settings.

g. (Optional) Activate the changes. Changes to credentials (badges) are downloaded to the Gateways on a regular schedule. To activate the changes before the next scheduled download, do one of the following.

- To immediately download the changes to the doors, select Hardware from the Doors menu, right-click on the Access GW Driver, and select Apply Credential Changes. This activates the changes on all doors. The badge is ready for use.

- To change the interval that credential changes are automatically downloaded to the doors, select System Configuration from the Admin menu, and then select Cisco Settings. In the field Credential download frequency (mins), enter the number of minutes between downloads. To activate changes to the Cisco Settings, you must restart the Cisco PAM appliance. See Cisco Settings, page 14-20 for more information.

Figure 8-5 Personnel Record: Badges General Window

Step 9 Click the Logins tab to edit the logins and profiles assigned to the person. Multiple login usernames can be associated with a personnel record.

a. From the main window for the Personnel record, click the Logins tab.

b. Click the Add... or Edit... button to open the Logins window, as shown in Figure 8-6.
Configuring Personnel

Figure 8-6 Personnel Record: Logins Window

- Complete the General settings. For field descriptions, see Creating User Login Accounts and Assigning Profiles, page 4-8.
- Complete the Profiles fields to define the access privileges for the login. For field descriptions, see Creating User Login Accounts and Assigning Profiles, page 4-8.
- Click Save and Close.

Step 10 Click the Custom tab to edit the custom-defined fields for the personnel record. This window includes text and date fields to hold information specific to an organization (see Figure 8-7).
Step 11  Click **Save and Close** in the **Personnel Record** window to make the changes permanent.
Chapter 8  Configuring Personnel and Badges

Downloading Credential Changes to the Gateway Modules

By default, any changes to user credentials are automatically downloaded (applied) to the Gateway modules every 60 minutes. If credential changes need to be downloaded sooner, use the Apply Credential Changes command on the Gateway driver. This command is useful if you want the changes to be immediately applied. For example, to immediately grant or deny user access to a door.

Procedure

Step 1  Select Hardware from the Doors menu.
Step 2  View the Credential Download Status.
   a. Select the Access GW Driver.
   b. Click the Credential Download Status tab in the Extended Status field, as shown in Figure 8-7.
   c. Click the box next to the Gateway name to show or hide additional information, including the following:
      - **Gateway Name**: the name of the Gateway module.
      - **Status**: the status of the download. For example: In Progress or Success.
      - **Time Stamp**: The time of the status change. For example, the time the download changed to In Progress or Success.

Figure 8-8  Personnel Record: Custom Window
Tip
To reapply the complete credential configuration for a specific Gateway, right-click the Gateway icon and select the Download All Credentials command. This command ensures the data is correct and should be used only if a problem exists.

Viewing Audit Records and Events for Personnel Records

This section describes how to view a list of audit records and events for personnel records.

Audit records are generated when a record is added, deleted, or modified, and display information about the change. Events are records of actions, such as attempts to gain access to an access point.

This section includes the following information:

- Viewing Audit Records, page 8-11
- Viewing Recent Events, page 8-13

Viewing Audit Records

Step 1 Select Personnel from the User menu.
Step 2 Double-click an entry (or select the entry and click Edit).
Step 3 Select Audit Records, as shown in Figure 8-9.
Step 4 Double-click an entry to view details for the item. Table 8-4 describes the audit record fields.
Figure 8-9 Personnel Audit Records Window

Table 8-4 Personnel Module: Audit Records Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time and date when the modification occurred.</td>
</tr>
<tr>
<td>Time Received</td>
<td>The time and date when the modification was saved.</td>
</tr>
<tr>
<td>Site</td>
<td>The site where the modification occurred. A site is a single instance of a</td>
</tr>
<tr>
<td></td>
<td>Cisco PAM database.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of change.</td>
</tr>
<tr>
<td>Log code</td>
<td>An abbreviated code uniquely identifying the type of change.</td>
</tr>
<tr>
<td>Priority</td>
<td>A priority used for sorting events and alarms. Positive priorities are above</td>
</tr>
<tr>
<td></td>
<td>normal priority, while negative priorities are below normal priority. Zero</td>
</tr>
<tr>
<td></td>
<td>is normal.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the change.</td>
</tr>
<tr>
<td>Device</td>
<td>The workstation name where the modification occurred. Click View to display</td>
</tr>
<tr>
<td></td>
<td>details for the device where the change was made, including the IP address</td>
</tr>
<tr>
<td></td>
<td>of the workstation device.</td>
</tr>
<tr>
<td>Credential</td>
<td>The username used when the modification occurred. Click View to display and</td>
</tr>
<tr>
<td></td>
<td>revise details for the username.</td>
</tr>
<tr>
<td>Personnel record</td>
<td>The name of the operator associated with the modification (if the login was</td>
</tr>
<tr>
<td></td>
<td>associated with a personnel record at the time).</td>
</tr>
<tr>
<td>Data</td>
<td>Additional information about the modification.</td>
</tr>
</tbody>
</table>
Configuring Personnel and Badges

Chapter 8

Editing Organization and Department Lists

Personnel records include an organization and department for the user (see the Occupational section of Personnel configuration, as described in Configuring Personnel, page 8-2, Step 6).

To define the organization and department selections, do the following:

**Step 1** Select Organization from the Users menu, as shown in Figure 8-10.

### Viewing Recent Events

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

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

**Step 3** Select Recent Events.

**Step 4** Double-click an entry to view details for the item. Table 8-5 describes the fields. Use the View, Report and Filter buttons for increased functionality.

#### Table 8-5 Personnel Module: Recent Events Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time and date when the event occurred.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the event.</td>
</tr>
<tr>
<td>Device</td>
<td>The device associated with the event.</td>
</tr>
<tr>
<td>Address</td>
<td>The address of the device.</td>
</tr>
<tr>
<td>Personnel Record</td>
<td>The personnel record associated with the event.</td>
</tr>
<tr>
<td>Data</td>
<td>This field displays detailed information about the event, the exact value</td>
</tr>
<tr>
<td></td>
<td>and meaning of which depends on the type of event. This field is generally</td>
</tr>
<tr>
<td></td>
<td>for advanced or troubleshooting use. If the event is associated with an</td>
</tr>
<tr>
<td></td>
<td>attempt to gain access to an access point using a badge that is not in the</td>
</tr>
<tr>
<td></td>
<td>database, this field contains the card number.</td>
</tr>
<tr>
<td>Credential</td>
<td>If the event has an associated credential (such as a badge or login), the</td>
</tr>
<tr>
<td></td>
<td>identifying information of the credential (such as a card or username) is</td>
</tr>
<tr>
<td></td>
<td>displayed in this field.</td>
</tr>
<tr>
<td>Site</td>
<td>The site where the event occurred.</td>
</tr>
</tbody>
</table>

### Editing Organization and Department Lists

Personnel records include an organization and department for the user (see the Occupational section of Personnel configuration, as described in Configuring Personnel, page 8-2, Step 6).

To define the organization and department selections, do the following:

**Step 1** Select Organization from the Users menu, as shown in Figure 8-10.
Chapter 8  Configuring Personnel and Badges

Editing Organization and Department Lists

Figure 8-10  Organizations: Main Window

Step 2  Select one of the following options:
- To add a personnel record, choose **Add**....
- To modify an existing record, select the entry and click **Edit**. You can also double-click the entry.
- To delete an entry, select the item and click **Delete**.

Step 3  If adding or editing an item, the **General** window appears, as shown in Figure 8-11.

Figure 8-11  Organizations: General Settings

Step 4  Enter the name of the organization an optional comments to describe the entry.

Step 5  Click the **Department** tab to edit the list of departments for the organization (Figure 8-12).

Step 6  Click **Add** to create a new department entry. To edit an entry, select the item and click **Edit**, or double-click the entry. To delete an item, select the item and click **Delete**.
Step 7 Click **Save and Close** to return to the main window.

Step 8 Click **Save and Close** again to save the organization and department changes and close the main window.

---

### Importing Personnel Records Using a Comma Separated Value (CSV) File

Large amounts of personnel records can be added to Cisco Physical Access Manager using a Comma Separated Value (CSV) file. A CSV file can be extracted from all common database vendors. This is the recommended method for the initial transfer of records into Cisco PAM.

**Before You Begin**

Review the following notes before creating EDI projects:

- To avoid system delays, do not import more than 5,000 personnel records at a time. If necessary, create multiple import files of less than 5,000 records each, and then import each file.
- Personnel records are unique based on the ID number of the record. If a record is imported with the same ID number, then the current record is overwritten with the new data.
- When organization and department values are included in an imported personnel record, those values must already exist in the Cisco PAM configuration. Add the Organization values by manually creating them or through a data import. See **Editing Organization and Department Lists, page 8-13** for more information.

Once a personnel CSV file is extracted from a database it can be added to Cisco PAM using the following process:

**Step 1** Enable the CSV personnel import wizard.

a. Select **System Configuration** in the Admin menu.

b. Select the **Data Entry/Validation - Personnel** tab (Figure 8-13).
Figure 8-13 Data Entry/Validation - Personnel

- System Configuration - Cisco Physical Access Manager
- Data Entry/Validation - Personnel

- LDAP
  - Password Policy
- Events/Alerts
  - Data Entry/Validation - Personnel
- Custom Personnel Fields
- Custom Device Fields
- Custom Badge Fields
- Personnel ID Number Generator
- PIN Generator
- Card Number Generator
- Support Contact Information
- Miscellaneous
- Cisco Settings

- Use CSV personnel import wizard

- Data Entry/Validation - Personnel

- Default personnel ID specifier
- Use CSV personnel import wizard

- System Configuration - Cisco Physical Access Manager
- Data Entry/Validation - Personnel

- Use CVS personnel import wizard

- System Configuration - Cisco Physical Access Manager
- Data Entry/Validation - Personnel

- Use CSV personnel import wizard

- Step 2 Select Personnel from the User menu.
- Step 3 Select CSV Import Wizard... from the Add... button drop-down menu (Figure 8-14).

Figure 8-14 CSV Import Wizard

- Click the Browse... button and locate the CSV file.
- Select the checkbox for File has a header row if the CVS file includes data for a header row.
- Select a file for Rejected records output file.
- Click Next.

- Step 4 In the File Selection window, select the file to import into Cisco PAM, as shown in Figure 8-15.
  - Click the Browse... button and locate the CSV file.
  - Select the checkbox for File has a header row if the CVS file includes data for a header row.
  - Select a file for Rejected records output file.
  - Click Next.

- Step 4 In the File Selection window, select the file to import into Cisco PAM, as shown in Figure 8-15.
  - Click the Browse... button and locate the CSV file.
  - Select the checkbox for File has a header row if the CVS file includes data for a header row.
  - Select a file for Rejected records output file.
  - Click Next.
Step 5  In the Column Configuration window (Figure 8-16), the top window contains entries from the CSV file with generic column headings such as Column 1, Column 2, etc. The bottom left-hand window displays the currently select column number in the CSV file and the name of the CSV field.
The header row entry will be blank if the **File has header row** check box is not checked in the previous step. The bottom right-hand of the window, labeled **Import as**: contains field names from the Cisco PAM database.
Assign a Cisco PAM field for each CSV field to be imported (Figure 8-16). Personnel records are unique based on the ID number of the record. If a record is imported with the same ID number, then the current record is overwritten with the new data.

a. Select a CSV column in the top window. By default, Column 1 will be selected, as is shown by the diamond symbol to the left of the column name.

b. Select the **Import as** field in the lower right-hand window. This defines the Cisco PAM field that corresponds with the selected CSV field.

c. Assign all CSV columns to an **Import as** field.

c. Click **Next**. The **Next** button is not enabled until all CSV fields are assigned.

**Note**

Personnel photos in the `.jpg` format can be imported. The CSV field assigned to the Cisco PAM photo field must contain the name of the photo file. In Windows, if a fully qualified path is not specified in the CSV field (e.g. `c:\photos\123456789.jpg`) then the location of the photos will be assumed to be on the desktop (e.g. `C:\Documents and Settings\Desktop\123456789.jpg`).

**Step 6**

In the Preview window, verify the records and fields before importing, as shown in **Figure 8-17**.

**Figure 8-17 CSV Preview**

![CSV Preview](image_url)
• **New Records** and **Updated Records** tabs: Select of deselect the checkbox to include or exclude the personnel record from the import.
  - Click **View** to display a preview of the imported personnel record that will be created.
  - Click **Back** to revise the settings if necessary.
• **Invalid Records** tab: displays personnel records that cannot be imported, including the reason for the failure.
  - Click **Export** to save the invalid records to a CSV file so they can be modified and re-imported.
  - The export file is defined in the File Selection screen (see Step 4). Click **Back** to revise the settings if necessary.

**Step 7** Click **Finish** to complete the import and add the personnel records to the system.

## Configuring Badges

Badges are assigned to personnel records. Use badge templates to define common settings for badge types. In the personnel record, select the badge template to quickly populate the badge fields, and then make additional changes, if necessary.

This section includes the following information.

- Configuring Badge Templates, page 8-20
- Badge Properties, page 8-22
- Using the Badge Designer, page 8-28
- Printing Badges, page 8-35

**Tip** Use the Personnel module to assign badges. Use the Badges module to view a summary of all the badges in the system, or to assign unassigned badges. Use the optional Badge Designer to create custom designs for your badges.

## Configuring Badge Templates

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select Badge Templates from the User menu.</td>
<td><img src="image" alt="Badge Templates Display" /></td>
</tr>
</tbody>
</table>
### Configuring Badges

#### Chapter 8  Configuring Personnel and Badges

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Click <strong>Add</strong>, or select an existing template and click <strong>Edit</strong>.</th>
</tr>
</thead>
</table>
| Step 3 | a. Enter the template name.  
          b. Click **Edit Template**. |
| Step 4 | a. Enter the badge properties. See **Badge Properties**, page 8-22 for field descriptions.  
          b. Click **OK** |
| Step 5 | Click **Save and Close**. The template is listed in the main window. |


## Badge Properties

This section describes the badge menus and settings. These settings are available in the Personnel, Badge Template, and Badges windows.

- Use the Personnel module to create and assign badges.
- Use Badge Templates to create pre-configured templates of common settings.
- Use the Badges module to view a summary of all the badges in the system or to assign unassigned badges.

This section includes the following information:

- Badges Module: General, page 8-22
- Badges Module: Cisco Access Policy, page 8-24
- Badges Module: Advanced Gateway, page 8-25
- Badges Module: Audit Records, page 8-27
- Badges Module: Recent Events, page 8-27

### Badges Module: General

The General tab includes basic information about the badge.

**Table 8-6**  
**Badges Module: General Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card #</td>
<td>(Required) Also known as a badge. A type of credential encoded with a card number, generally on a magnetic stripe or internally like a proximity card, and used to enter access points.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> If unsure what the card # is on the card, use the card in the access-control system reader. Open the Events module and view the event with the description Access denied: Card not in database. The Data field of the event displays the card number read from the card. See Viewing Audit Records and Events for Personnel Records, page 8-11.</td>
</tr>
<tr>
<td>PIN</td>
<td>(Required) Personal Identification Number. A badge has a PIN associated with it, which, depending on the configuration of an access point, is entered into the keypad on the access point's reader.</td>
</tr>
<tr>
<td>Hot stamp</td>
<td>(Optional) The number physically printed or embossed on a badge. This number is generally independent of the Card Number. Not all badges have a hot stamp number.</td>
</tr>
<tr>
<td>Facility code</td>
<td>(Optional) A segment of bits encoded on a card that represent a number for a facility. Often all cards issued for a single facility have the same facility code.</td>
</tr>
<tr>
<td>Exempt from Anti-passback</td>
<td>(Optional) If the access point is configured for anti-passback, the badge is exempt from anti-passback enforcement.</td>
</tr>
<tr>
<td>Grant One Free APB Pass</td>
<td>(Optional) The badge holder will be anti-passback exempt during the next reader use only.</td>
</tr>
</tbody>
</table>
### Table 8-6  Badges Module: General Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Badge Type</strong></td>
<td>The type of badge. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Standard</td>
</tr>
<tr>
<td></td>
<td>• Temporary</td>
</tr>
<tr>
<td></td>
<td>• Visitor</td>
</tr>
<tr>
<td><strong>Assigned to</strong></td>
<td>(Optional) The personnel record the badge is assigned to.</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td>(Optional) The current status of the badge. Only the <strong>Active</strong> option provides access for the badge. The options include:</td>
</tr>
<tr>
<td></td>
<td>• Active: Must be set to this value for access to be granted.</td>
</tr>
<tr>
<td></td>
<td>• Inactive: Access is denied for all access points in system.</td>
</tr>
<tr>
<td></td>
<td>• Lost: Access is denied for all access points in system.</td>
</tr>
<tr>
<td></td>
<td>• Stolen: Access is denied for all access points in system.</td>
</tr>
<tr>
<td></td>
<td>• Destroyed: Access is denied for all access points in system.</td>
</tr>
<tr>
<td><strong>Effective</strong></td>
<td>(Optional) The beginning date the badge can be used in the system. If blank, badge access begins immediately.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If a date is entered, the badge can be used at 12.00 AM on the specified day.</td>
</tr>
<tr>
<td><strong>Expires</strong></td>
<td>(Optional) The date the badge expires. If blank, the badge never expires.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If a date is entered, the badge expires at 12.00 AM on the specified day.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>(Optional) A site is a single instance of a Cisco PAM database.</td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>(Optional) Any additional comments or notes about the badge.</td>
</tr>
</tbody>
</table>
Badges Module: Cisco Access Policy

Select the door access policies for the user badge. See Configuring Access Policies, page 9-2.

Figure 8-18  Badges: Cisco Access Policy Selection
Badges Module: Advanced Gateway

Table 8-7 describes the advanced settings for the Cisco Physical Access Gateway.

**Table 8-7  Badges Module: Advanced Gateway Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential template ID</td>
<td>The Credential Template for the badge. This allows the badge to be recognized by the Cisco Physical Access Gateway as a valid badge. See Configuring Credential Templates, page 7-17 for more information.</td>
</tr>
<tr>
<td>Temporary deactivation date</td>
<td>(Optional) The start date to temporarily deactivate a badge. Click on the entry field to open a pop-up calendar, and then double-click to select a date. For example, to deactivate a badge for a one-week vacation beginning January 1, select the date from the pop-up calendar, and then enter 7 in the following duration field. If a date is entered, the badge deactivation begins at 12.00 AM on the specified day.</td>
</tr>
<tr>
<td>Temporary deactivation duration</td>
<td>(Optional) The duration of the temporary deactivation, in days. For example, to deactivate a badge for a 7 day vacation, enter 7.</td>
</tr>
<tr>
<td>Use limit</td>
<td>(Optional) The maximum number of times a badge can be used. When the limit is reached, the badge is deactivated.</td>
</tr>
<tr>
<td>Role</td>
<td>(Optional) The role of the person who carries the badge: Employee, Contractor, Vendor, or Temporary.</td>
</tr>
<tr>
<td>Executive credential</td>
<td>If checked, specifies that the badge belongs to an executive.</td>
</tr>
<tr>
<td>PIN exempt</td>
<td>If checked, the badge holder is not required to enter the PIN for a reader in Card and PIN mode.</td>
</tr>
<tr>
<td>ADA access enable</td>
<td>If checked, the badge will use the ADA door strike time, allowing the badge holder more time to pass.</td>
</tr>
</tbody>
</table>
Chapter 8  Configuring Personnel and Badges

Badges Module: HSPD-12 Badge Extension

Table 8-7 describes the HSPD-12 Smart Card badge extension settings.

Note

The HSPD-12 badge extension is experimental and may be changed or removed in future Cisco PAM releases. For this reason, the extension should not be used in a production setting.

Table 8-8  Badges Module: HSPD-12 HSPD-12 Badge Extension Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Code</td>
<td>Identify the government agency issuing the credential.</td>
</tr>
<tr>
<td>Site Code</td>
<td>Identifies the site code associated with the credential.</td>
</tr>
<tr>
<td>Credential Number</td>
<td>The number encoded by the issuing agency. Only one credential number can be active in a system.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date the credential expires and is deemed invalid.</td>
</tr>
<tr>
<td>Card Type</td>
<td>The specified Smart Card credential type. The currently supported type is PIV.</td>
</tr>
<tr>
<td>FASC -N</td>
<td>The Federal Agency Smart Credential Number. This data is in the BCD (binary encoded data) format and is comprised of fields such as Agency Code, System Code, Credential Number, Credential Series, Individual Credential Issue code, and other fields.</td>
</tr>
<tr>
<td>Credential series</td>
<td>Credential series code used to reflect major system changes.</td>
</tr>
<tr>
<td>System code</td>
<td>Identifies the system that issued the card.</td>
</tr>
<tr>
<td>ICI</td>
<td>Individual Credential Issue code. Initially it is set to 1 and incrementally increased by 1 if the card is replaced, damaged, or lost. For example, the ICI for a replacement card would be 2.</td>
</tr>
<tr>
<td>CRL initial date</td>
<td>Date when the CRL (Certificate Revocation List) was first updated.</td>
</tr>
<tr>
<td>CRL latest date</td>
<td>Date when the CRL (Certificate Revocation List) was last updated.</td>
</tr>
<tr>
<td>Transport PIN</td>
<td>The PIN code associated with the credential.</td>
</tr>
<tr>
<td>CUID</td>
<td>The Card Holder Unique Identifier.</td>
</tr>
<tr>
<td>Full name</td>
<td>The full name of the card holder.</td>
</tr>
<tr>
<td>SHA -1 hash</td>
<td>The SHA-1 Hash Code of the FASC-N.</td>
</tr>
</tbody>
</table>
Badges Module: Audit Records

When an operator adds, deletes, or modifies a record, an audit record is generated. The following information is included in each audit record:

Table 8-9 Badges Module: Audit Records Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time and date when the modification occurred.</td>
</tr>
<tr>
<td>Time Received</td>
<td>The time and date when the modification was saved in the application.</td>
</tr>
<tr>
<td>Site</td>
<td>The site where the modification occurred.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of change made.</td>
</tr>
<tr>
<td>Log code</td>
<td>An abbreviated code uniquely identifying the type of change.</td>
</tr>
<tr>
<td>Priority</td>
<td>A priority used for sorting events and alarms. Positive priorities are above normal priority, while negative priorities are below normal priority. Zero is normal.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the modification: what type of record was modified, and whether it was inserted, updated, or deleted.</td>
</tr>
<tr>
<td>Device</td>
<td>The name of the workstation device where the modification occurred.</td>
</tr>
<tr>
<td>Address</td>
<td>The address of the workstation device where the modification occurred.</td>
</tr>
<tr>
<td>Credential</td>
<td>The login that the operator was logged in with when the modification occurred.</td>
</tr>
<tr>
<td>Personnel record</td>
<td>The name of the operator associated with the modification, if the login was associated with a personnel record at the time.</td>
</tr>
<tr>
<td>Data</td>
<td>Additional information about the modification.</td>
</tr>
<tr>
<td>View Current...</td>
<td>Opens a new window displaying the current settings.</td>
</tr>
<tr>
<td>View Before...</td>
<td>Opens a new window displaying the settings before the change was made.</td>
</tr>
<tr>
<td>View After...</td>
<td>Opens a new window displaying the settings after the change was made.</td>
</tr>
</tbody>
</table>

Badges Module: Recent Events

Lists the recent events of the selected badges. Use the View, Report and Filter buttons for increased functionality. The following fields are listed in the recent events list:

Table 8-10 Badges Module: Recent Events Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time and date when the event occurred.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the event.</td>
</tr>
<tr>
<td>Device</td>
<td>The device associated with the event.</td>
</tr>
<tr>
<td>Address</td>
<td>The address of the device.</td>
</tr>
<tr>
<td>Personnel Record</td>
<td>The personnel record associated with the event.</td>
</tr>
</tbody>
</table>
Using the Badge Designer

Use the **Badge Designer** to create and modify badge designs, as described in the following instructions.

<table>
<thead>
<tr>
<th>Step 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>Badge Designer</strong> from the Admin menu. The main window of the <strong>Badge Designer</strong> module displays all badge templates loaded into the system.</td>
</tr>
</tbody>
</table>

**Note**

This feature requires an optional Cisco license. The **Badge Designer** menu appears only after the license is installed on the Cisco PAM server. See **Obtaining and Installing Optional Feature Licenses**, page 2-21 for more information.

---

**Table 8-10**  
**Badges Module: Recent Events Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.</td>
</tr>
<tr>
<td>Credential</td>
<td>If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.</td>
</tr>
<tr>
<td>Site</td>
<td>The site where the event occurred.</td>
</tr>
</tbody>
</table>
Step 2  Do one of the following:

- View or modify an existing template:
  - Click an existing template name to view details of the template. Click the Front and Back tabs in the design window to view both sides of the badge template. Select the checkbox **Preview Sample Data** to preview the badge template with sample data, if included in the template design.
  - Click **Properties...** to edit the name and size of the badge template. Skip to **Step 4** for instructions.
  - Click **Design...** to edit the graphic design of the badge template. Skip to **Step 6** for instructions.
  - Click **Duplicate...** to create a duplicate of the badge template.
  - Click **Delete...** to delete the badge template.
  - Click **Print...** to print a test badge template.
  - Click **Add...**: to add a new badge template, as described in the following steps.

Step 3  To create a new template, click **Add...** to open the **SVG Badge Format** window, as shown in **Figure 8-20**.

**Figure 8-20  New Badge Format**

Step 4  Enter the template properties:

a. **Name**: Enter a descriptive name.

b. **Format**: Select if the badge is single sided or double sided.

c. **Orientation**: portrait or landscape.

d. **Card Size**: Select a standard size, or enter custom dimensions. Standard size options include:
   - CR-80 Flush Cut 54 x 85.7mm
   - CR-80 Lip Seal 48 x 80mm
   - Badge 67 x 98mm
   - Badge 79 x 99mm
Tip
To modify an existing template, select the template name from the main window and click Design button. To edit the properties for an existing template, click the Properties button.

Step 5
Click OK. The Badge Format Editor opens in the format, orientation, and size configured in Step 4. For two-sided badges, there is a separate window for the front and back of the templates, as shown in Figure 8-21.

Figure 8-21 Badge Format Editor

Step 6
Use the Tool Bar icons at the top of the window to design the template. The icons include the following tools (from left to right):

Tip
Hold the mouse cursor over an icon to view the icon title.

- **Color**: Click the icon to select a color and then drag and drop the color on a shape to apply that color.
- **Mouse Pointer Tool**: Select and move objects on the badge template.
- **Rectangle Tool**: Draw rectangle objects.
- **Circle Tool**: Draw a circle.
Ellipse Tool: Draw an ellipse.
Line Tool: Draw a line.
Polygon Tool: Draw a polygon.
Polyline Tool: Draw an a polygon with operator defined line lengths.
Text: Add text to the template.
Image: Add an image to the template.
Quadratic Bezier Curve: Create a line between 3 points.
Cubic Bezier Curve: Create a line between 4 points.
Color Picker Tool: Select a color from the palette.
Image Link: Create an image link to the Cisco PAM database. Options include: personnel photos or signatures.
Text Link: Create a text link to the Cisco PAM database. Options include: Personnel and Badge Manager fields.
Properties: Properties available for the selected object.
Resources: Resources of the selected object.

Step 7  Draw a rectangle, as shown in Figure 8-22.

Figure 8-22  Badge Format Editor: Rectangle Tool

a. Click the rectangle button in the tool bar and drag a rectangle on the badge template.
b. To edit the colors of the rectangle, click the Color button on the left side of the Tool Bar.

Step 8  Select a stroke color for the badge. The stroke is the outline of the rectangle.
c. Select the rectangle on the badge template to display blue arrows at each corner.

d. In the **Properties** section select the **Stroke** tab.

e. With the **Color** radio button selected use the **Color picker** and choose a desired stroke color.

f. Select an appropriate width value. The **Width** field increases the size of the stroke.

g. Press **Enter** or click outside of the field to apply the setting.

**Step 9** Select a fill color for the badge. The fill is the color of the rectangle.

a. Click the **Normal** button (displayed as an arrow) in the **Tool Bar**.

b. Select the rectangle on the badge template. The rectangle is displayed with blue arrows at each corner.

c. In the **Properties** section select the **Fill** tab.

d. With the **Color** radio button selected use the **Color picker** and choose a desired fill color.

e. Press **Enter** or click outside of the field to apply the setting.

**Step 10** Add a logo to the badge template:

a. Click the **Image** button.

b. On the template, click and drag a rectangle at a desired location for the logo to open the image browser.

c. Select a valid file type (.jpg, .png, and .svg) on a local drive and click **Open**. The logo appears in the box, as shown in **Figure 8-23**.

d. Click and drag the logo to a desired location.

**Figure 8-23**  **Badge Format Editor: Logo**
Step 11  To add a dynamic text field to the badge template:
   a. Click the Text Link button in the Tool Bar.
   b. In the Properties section select the Database Text Link tab, as shown in Figure 8-24.
   c. In the field drop-down select the correct text link. This text link extracts the field from the database. For example the Title text link field extracts the personnel title from the database.
   d. (Optional) In the Properties section select the other attributes of the text, such as size and font.
   e. Click and drag the text to a desired location.

Figure 8-24  Badge Format Editor: Database Text Link

Step 12  To add a dynamic image to the badge template:
   a. Click the Image Link button in the Tool Bar.
   b. Click and drag a rectangle on the badge temptingly where the image will appear.
   c. In the Properties section select the Database Image Link tab.
   d. In the field drop-down select Photo, as shown in Figure 8-25. This object extracts the photo from the personnel database.
   e. Click and drag the box to a desired location.

Tip
Select Optimize Images from the File menu to resize all photos to the area they occupy on the badge. If the photos do not optimize with sufficient resolution, you may need to manually resize photos in an external photo editor to achieve the best possible print quality. See Printing High Resolution Images, page 8-40 for more information.
Figure 8-25  Badge Format Editor: Database Image Link

**Step 13**  Click the File button and select **Save All** to save changes.

**Step 14**  Click the File button and select **Exit** to close the **Badge Format Editor**. The new template appears in the **Badge Designer**, as shown in Figure 8-25.

Figure 8-26  Badge Designer With New Template
Printing Badges

To print badges, you must first assign a format to the badge (badge formats are the designs created using the badge designer, as described in Using the Badge Designer, page 8-28). Once the badge is assigned a design, you can print badges individually, or in groups.

Note
- To print badges, you must first purchase and install the Badge Designer license. See Obtaining and Installing Optional Feature Licenses, page 2-21 for instructions.
- To print multiple badges at once, you must also enable the batch printing feature. See Printing Multiple Badges, page 8-36 for instructions.

This section includes the following information:
- Printing Individual Badges, page 8-35
- Printing Multiple Badges, page 8-36
- Printing High Resolution Images, page 8-40
- Changing the Default Badge Printer, page 8-40
- System Configuration Settings for Badge Printing, page 8-41

Printing Individual Badges

To print a single badge, do the following:

Step 1  Purchase and install the Badge Designer license to enable badge printing. See Obtaining and Installing Optional Feature Licenses, page 2-21 for instructions.

Step 2  (Optional) Create the badge formats (designs), as described in Using the Badge Designer, page 8-28. You can also use one of the designs included with Cisco PAM.

Step 3  To define a badge format for a single badge, do the following:
  a.  Select Badges from the User menu.
  b.  Right-click a badge and select Edit from the drop-down menu.
  c.  Click the Badge Printing tab and select a Format, as shown in Figure 8-27.
  
  Note  The Badge Printing tab appears only after the optional Badge Designer license is installed.
  d.  Click Print.

Tip  If a format is already assigned for the badge, you can print from the main window. Click to highlight the badge, and then select Print Selected Items from the Print menu. If a format is not defined, however, the print job will fail. To view the status of print jobs, select Batch Badge Printing from the User menu.
Step 4 Configure a default printer, as shown in Figure 8-27.

These steps only occur if a default printer is not configured.

a. Click Yes to configure the default printer. This defines the printer used to print Cisco PAM badges.

b. In the Select print configuration window, select Create new configuration.

c. In the Print window, select a printer, and click OK.

d. In the Page Setup window, adjust the settings if necessary, and click OK.

e. Enter a name for the printer configuration and click OK. For example: USB Printer.

f. Wait for the badge to print on the selected printer. To view the status in the print job, select Batch Badge Printing from the Admin menu.

Printing Multiple Badges

To print multiple badges at once, do the following:

Step 1 Purchase and install the Badge Designer license to enable badge printing. See Obtaining and Installing Optional Feature Licenses, page 2-21 for instructions.

Step 2 (Optional) Create the badge formats (designs), as described in Using the Badge Designer, page 8-28. You can also use one of the designs included with Cisco PAM.

Step 3 Enable batch badge printing.

a. Select System Configuration from the Admin menu.

b. Select Data Entry/Validation - Badge, as shown in Figure 8-28.

c. Uncheck the Disable batch badge printing box.

d. Exit and re-launch the Cisco PAM application to activate the setting.
Step 4 Define the format for the badges to be printed.

Tip If a format is already assigned for all of the selected badges, skip to Step 5. Check the Format column to view the assigned format, if any (Figure 8-29).

a. Select Badges from the User menu.

b. (Optional) Shift-click or control-click to select multiple badges.

c. Click the Group Edit menu and select Group Edit All Items or Group Edit Selected Items from the drop-down menu (Figure 8-29).
d. Click the **Badge Printing** tab and check the **Format** check box, as shown in *Figure 8-30*.
e. Select a format and click **OK**.

**Figure 8-30  Badge Printing Format for Multiple Badges**

![Badge Printing Format for Multiple Badges](image)

**Note** Badge Printing appears only if the optional Badge Designer license is installed.

**Step 5** Print the badges.

**Note** If a format is not assigned for any of the selected badges, as described in *Step 4*, the print job will fail. To view the status of print jobs, select **Batch Badge Printing** from the **User** menu.

a. Select **Badges** from the **User** menu, if necessary.
b. Shift-click or control-click to select multiple badges.
c. Click the **Print** menu and select **Print All Items** or **Print Selected Items** from the drop-down menu (Figure 8-31).

**Figure 8-31  Printing Multiple Badges**

![Printing Multiple Badges](image)

**Step 6** (Optional) Configure a default printer, as shown in *Figure 8-27 on page 8-36*. These steps only occur the first time you print a badge.

a. Click **Yes** to configure the default printer. This defines the printer used to print Cisco PAM badges.
b. In the Select print configuration window, select Create new configuration.

c. In the Print window, select a printer, and click OK.

d. In the Page Setup window, adjust the settings if necessary, and click OK.

e. Enter a name for the printer configuration and click OK. For example: USB Printer.

**Tip**
To change the default printer, see Changing the Default Badge Printer, page 8-40.

**Step 7**
Select a Batch Printing Option, as shown in Figure 8-32.

**Figure 8-32 Batch Printing Options**

- Select Print Now to print the badges immediately.
- Select Print Later and enter a Date and Time to automatically print the badges later.
- Click OK to print the badges.

**Step 8**
To view the status of the print job, do the following:

a. Select Batch Badge Printing from the Admin menu, as shown in Figure 8-33.

**Figure 8-33 Batch Badge Printing Status**

b. Highlight the print job, and click Edit.

c. Select Batch Items in the Badge Print Batch window to view the items included in the print job.
### Printing High Resolution Images

The highest possible photo print quality is achieved when the resolution of the photo matches the print resolution of the printer: the target width and height of the photo should be multiplied by the printer resolution.

For example, if you are using a 300 dpi (dots-per-inch) printer, the ideal photo resolution that will occupy a 1” x 1” area is 300 x 300 pixels, a 2” x 2” area is 600 x 600 pixels, and a 2” x 3” area is 600 x 900 pixels.

Mathematically, the ideal resolution can be calculated as \((rX, rY) = (w \times \text{DPI}, h \times \text{DPI})\) where:

- \((rX, rY)\) is the resolution of the photo
- \(rX\) is the number of pixels in width
- \(rY\) is the number of pixels in height
- \(w\) is the target width of the image on the badge
- \(h\) is the target height of the image on the badge
- \(\text{DPI}\) is the resolution (dots-per-inch) of the printer

The **Badge Format Editor** includes a function to automatically optimize images.

1. Select **Badge Designer** from the **Admin** menu.
2. Click the Design button to open the **Badge Format Editor**.
3. Select **Optimize Images** from the **File** menu to resize all photos in the template to the area they occupy on the badge.

**Note**

If the photos do not optimize with sufficient resolution, you may need to manually resize photos in an external photo editor to achieve the best possible print quality.

### Changing the Default Badge Printer

The default printer is configured when you print a badge. Complete the following instructions to remove the default printer and select a new printer.

**Step 1** Select **Preferences** from the **Options** menu.

**Step 2** Click the **Badge Printers** tab.

**Note** Badge Printers appears only after the Badge Designer license is installed.

**Step 3** In the Configurations section, select the printer that displays **Badge: Badge Printing** in the **Applies to** section, as shown in Figure 8-34.
Step 4  Select **Badge: Badge Printing** and click **Remove**.

Step 5  Click **OK** to save the changes and close the window.

Step 6  To set a new default printer, print a badge as described in **Printing Individual Badges, page 8-35** or **Printing Multiple Badges, page 8-36**. When printing, you will be prompted to select a new default badge printer.

---

**System Configuration Settings for Badge Printing**

Options for badge printing are available in two System Configuration screens:

- **Data Entry/Validation - Badge**
- **Miscellaneous**

This section describes the settings and options available in each window.

---

Step 1  Select **System Configuration** from the Admin menu.

Step 2  Select **Data Entry/Validation - Badge** (Figure 8-35).
Figure 8-35   Badge Printing Options in Data Entry/Validation - Badge

Step 3  Select or deselect one or more of the following options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow printing of unsaved badges</td>
<td>Allows printing new badges before the badge is saved. For highest security, leave this unchecked. When allowed (which may be more convenient), it is possible to print a badge without having any record of the badge.</td>
</tr>
<tr>
<td>Disable batch badge printing</td>
<td>Enables or disables the batch printing module. See Printing Multiple Badges, page 8-36.</td>
</tr>
</tbody>
</table>
Step 4 Select the Miscellaneous tab (Figure 8-36).

Figure 8-36 Badge Printing Options in the Miscellaneous Settings

Step 5 Select or deselect one or more of the following options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use cross-platform page setup dialog for badge printing</td>
<td>Select this option to use the cross-platform Java page dialog if the badge image is truncated. This occurs when using the default printer dialog on some printers (such as the Zebra printer).</td>
</tr>
<tr>
<td>Truncate imageable area values used to initialize cross-platform page dialog</td>
<td>If the image is still truncated using the cross-platform Java page dialog, select this option to apply .01 inch margins.</td>
</tr>
<tr>
<td>Use Pageable print interface for badge printing</td>
<td>The Java Printable printing interface is used by default. If printing problems occur (such as with the Evolis printer), select this option to use the Java Pageable printer interface.</td>
</tr>
<tr>
<td>Stroke text before printing badges</td>
<td>If problems occur printing text, such as on a Mac, select this option to apply a stroke when printing.</td>
</tr>
</tbody>
</table>

Step 6 Click Save to save the changes.

Step 7 Restart Cisco PAM (exit and relaunch the application) to activate the changes.

Note Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Setting Up Image and Signature Options for Personnel Records

To add images and signatures to personnel records, enable the features as described in this section:

- Enabling Image Capture Devices
- Enabling Signature Capture Devices

Enabling Image Capture Devices

Cisco PAM supports capture devices (badging cameras) that use TWAIN drivers. Before proceeding to the steps below, install all necessary camera drivers including TWAIN drivers. If unsure if the camera uses a TWAIN driver contact the camera manufacturer for assistance.

**Step 1** Select Preferences from the Options menu.

**Step 2** Select the Image Capture tab on the left of the Preferences window, as shown in Figure 8-37.

**Step 3** Check the Is present checkbox.

**Step 4** Select the image capture device type from the Type: drop-down menu. The options are:

- Video
- TWAIN

**Step 5** Click the Select TWAIN source from the list button to open a source window. All selected drivers installed on the machine will be displayed. Select the correct driver and click the OK button.

**Step 6** If necessary modify the image width, height and scale of the capture device using the following settings.

- Final image width: The pixel width of the image capture.
- Final image height: The pixel height of the image capture.
- Preview image scale: The size of the image preview.
- Crop height scale: It's recommended that the crop height and final image height are equal.
Enabling Signature Capture Devices

Step 1 Select System Configuration from the Admin menu.

Step 2 Select the Data Entry/Validation - Personnel tab at the left of the window, as shown in Figure 8-38.

Figure 8-38  System Configuration: Personnel Data Entry Window

Step 3 Check the Use signature capture box. Checking this box enables the signature capture capability in the Personnel module.

Step 4 Click Save to save the changes.

Step 5 For system configuration changes to take effect, restart the Cisco PAM application.

Note You must exit and re-launch the Cisco PAM application for the changes to take effect. The Signature Capture menu in the Preferences window does not appear until the application is restarted.

Step 6 Log in to the Cisco PAM application.

Step 7 Select Preferences from the Options menu.

Step 8 Select the Signature Capture tab on the left of the Preferences window, as shown in Figure 8-39.
Step 9  Check the **Is Present** checkbox and the **Type** of signature pad from the drop-down. Select the communications port from the drop-down.

Step 10  Click **OK** to save the settings. The signature detail in the Personnel module now includes an **Import** and **Capture** button. See Configuring Personnel, page 8-2 for more information.
CHAPTER 9

Configuring Cisco Access Policies

This chapter describes how to create the Cisco Access Policies assigned to badge holders that define which doors they can access, and the dates and times of that access. Once created, access policies are assigned to personnel badges.

In addition, you can create access policy schedules for doors that define when the doors are available.

Contents

- Configuring Access Policies, page 9-2
- Managing Door Access With Access Control Policies, page 9-4
- Using the Schedule Manager, page 9-7
  - Modifying Types and Time Ranges, page 9-10
- Configuring Anti-Passback Areas, page 9-14
- Monitoring Anti-Passback Events, page 9-16
- Configuring Two-Door Policies, page 9-17
- Two-Door State Monitoring, page 9-19
### Configuring Access Policies

This section describes how to create an access policy and assign it to a user badge.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select <strong>Access Policy</strong> from the Doors menu, under the Access Policies sub-menu.</td>
<td>![Display showing Access Policy menu]</td>
</tr>
<tr>
<td><strong>Step 2</strong> Click <strong>Add</strong>, or select an existing entry and click <strong>Edit</strong>. <strong>Tip</strong> To remove a policy, highlight the entry and click <strong>Delete</strong>. Access policies cannot be deleted if they are assigned to one or more badges. Remove the policy assignment from all badges, and then delete the policy.</td>
<td>![Display showing Access Policy list]</td>
</tr>
</tbody>
</table>
| **Step 3** Enter the general information for the policy:  
  a. **Name**: Enter a descriptive name for the policy.  
  b. **Description**: Enter a description of the purpose or usage of the policy.  
  c. **Enabled**: Select the checkbox to enable or disable the policy. The policy is enabled by default. If disabled, the policy can be assigned to users, but will not impact the users’ access privileges. | ![Display showing Access Policy details] |
### Step 4
Add or remove sets of door and schedule settings for the access policy.

a. Select a door or door group from the list box on the left. You can change the doors listed using the following controls:

- **Search Door List:** Search for a specific door using one or more keywords.
- **Door / Door Group:** Select an option to display single doors or door groups in the list view.
  - See Chapter 6, “Configuring Doors” to add doors.
  - Door Groups allow you to create groups of doors, such as all lobby doors. See Configuring Device Groups, page 6-28.

b. Select a **Schedule.** To create a new schedule, click the **New Schedule** button. See Using the Schedule Manager, page 9-7 for information.

c. Repeat these steps to add or remove doors or schedules for the access policy.

d. Verify that the correct doors and schedules appear in the list box on the right: Door / Door Group and Schedule Pairs.

### Step 5
Click **Save and Close** to save the access policy.

### Step 6
Assign the access policy to one or more user badges:

a. Open the **Personnel** module from the Users menu.

b. Click **Add,** or select an existing personnel entry and click **Edit.**

c. Select the **Badges** sub-menu.

d. Click **Add,** or select an existing badge entry and click **Edit.**

e. Select **Cisco Access Policy** (in the Badge window).

f. Select the door access policies for the user badge.

g. Click **Save and Close** to close the Badge window.

h. Click **Save and Close** to close the personnel record.

**Tip** See Chapter 8, “Configuring Personnel and Badges” for more information.
Managing Door Access With Access Control Policies

Access Policies can be deactivated and activated manually for one or more doors. For example, if you create three access policies for lobby doors: one for employees, a second for contractors, and a third for visitors, you can selectively deactivate the access policy for contractors on the main lobby door, or on all doors.

Access policies remain deactivated until one of the following events occur:

Table 9-1   Reactivating Access Control Policies

<table>
<thead>
<tr>
<th>Command or action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Access Policies</td>
<td>Right-click a door and select the Activate Access Policies command to manually activate a policy that was deactivated. Select the policies to be activated from the pop-up window and click OK.</td>
</tr>
<tr>
<td>Reset Gateway</td>
<td>Right-click a Gateway icon and select the Reset Gateway command to perform a soft reset of the Gateway module. Access policies are activated during a soft reset.</td>
</tr>
<tr>
<td>Reload Gateway Configuration</td>
<td>Right-click a Gateway icon and select the Reload Gateway Command to replace the existing Gateway configuration with a new copy. Access policies are activated during this process.</td>
</tr>
<tr>
<td>Power cycle the Gateway module</td>
<td>Access policies are activated whenever a Gateway is powered up. For example, after a power failure or anytime power is disconnected and restored.</td>
</tr>
</tbody>
</table>

Procedure

Complete the following instructions to deactivate and reactivate door access policies:

To do this | Use this display
---|---
Step 1 View the status of access policies on a door:  
a. Select Hardware or Locations & Doors from the Doors menu.  
b. Click the door to highlight it.  
c. In the Extended Status field, click the Access Policies tab to view the policies and status for the door.
Step 2
To manually deactivate a policy, right-click the door icon and select **Deactivate Access Levels**.

**Tip**
To deactivate access policies for multiple doors, select the command from a location (Locations & Doors module) or from the Logical Driver (Hardware module).

Step 3
Select the access policies to deactivate and click **OK**.

**Tip**
Use Shift-click or Ctrl-click to select multiple items from the list.

Step 4
Verify that the status of the access policy is **No**:

a. Click the door to highlight it. This also refreshes the Extended Status data.

b. In the Extended Status field, click the Access Policies tab.

c. Confirm that the access policy is **No**.
### To do this

**Step 5** To reactivate the access level, right click the door icon and select **Activate Access Levels**. Select one or more levels from the list and click **OK**.

**Note** Access policies remain deactivated until manually reactivated using this command. See on page 9-4 for other methods to reactivate access control policies.
Using the Schedule Manager

The Schedule Manager defines schedules for users and doors, including the following:

- Access Policy schedules determine when a badge can be used to access doors. For example, you can create a basic access policy schedule for the weekdays, an additional schedule for the weekend, and a third that denies access for specified holidays when the building is closed. See Configuring Access Policies, page 9-2 for more information.

- Door schedules are used in door configurations to define the state of the door based on the time and day. For example, a door schedule can define a lobby door as being open and unlocked from 8 am to 5 pm, but locked all other hours. See Configuring Doors, page 6-2 for more information.

To add or edit schedules, do the following:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select Schedules from the Doors menu, in the Schedule Manager sub-menu.</td>
<td><img src="image1.png" alt="Schedule Manager" /></td>
</tr>
<tr>
<td><strong>Step 2</strong> Click Add, or select an exiting entry and click Edit. To remove a schedule, highlight the entry and click Delete. <strong>Note</strong> Schedules cannot be deleted if they are assigned to one or more access policies. To delete schedule that is assigned to an access policy, you must first remove the schedule assignment from all access policies.</td>
<td><img src="image2.png" alt="Schedule Manager - Cisco Physical Access Manager" /></td>
</tr>
<tr>
<td><strong>Step 3</strong> Enter the name and description for the schedule.</td>
<td><img src="image3.png" alt="Add - Schedules" /></td>
</tr>
</tbody>
</table>
Chapter 9  Configuring Cisco Access Policies

Using the Schedule Manager

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Select a Schedule Type:</td>
</tr>
<tr>
<td>– Door Policy: door schedules appear in the door Properties window under the menu: Door enable schedule. See Step 6, page 7-10 in Configuring Door Templates for more information.</td>
<td><img src="image1.png" alt="Add - Schedules" /></td>
</tr>
<tr>
<td>– Access Policy: access policy schedules define the schedule for user badge access. See Configuring Access Policies, page 9-2 for more information.</td>
<td><img src="image2.png" alt="Add - Schedules" /></td>
</tr>
</tbody>
</table>

**Step 5**

Select the Type, and then select an existing Value.

To create or modify the available values, see Modifying Types and Time Ranges, page 9-10.

- Select Holiday to define a single date, or range of consecutive dates.
- Select Work Weeks to define the days of the week for a schedule.
- Select Special Cases to define a schedule for a date or range of dates that repeat on a regular schedule. For example, the first Monday in each month.
- The Time Entry Collection allows you to reuse Holiday, Work Weeks, or Special Case schedules.

**Note**  
A Time Entry Collection can be used in more than one schedule, but only if the schedules have the same action (such as Allow or Deny). If a Time Entry Collection is assigned to schedules with different actions, then the schedule operation will be inconsistent.

**Step 6**

Select an Action:

- Access Policy schedules: select Deny or Permit to define if the user should have access during the defined schedule.
- Door schedules: select Use Schedule Mode.

**Note**  
The option Default Mode enables the default door mode defined in the door Properties window. See Step 6, page 7-10 in Configuring Door Templates for more information.
<table>
<thead>
<tr>
<th>Step</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
</table>
| 7    | Select a **Time Range** for the schedule.  
To create or modify the available values, see **Modifying Time Ranges**, page 9-11. | ![Schedule Manager](image) |
| 8    | Click **Add** to add the entry to the list of defined schedules. | ![Add Schedule](image) |
| 9    | a. Repeat **Step 5 to Step 9** to add additional schedules, if necessary.  
b. Click **Save and Close**. | ![Schedule Manager](image) |
| 10   | To apply schedules to an access policy, see **Configuring Access Policies**, page 9-2.  
To apply a schedule to a door configuration, see **Configuring Door Templates**, page 7-7 and **Configuring Doors**, page 6-2. Door schedules are selected in the Properties window, in the **Use Schedule Mode** menu. | ![Schedule Manager](image) |
Modifying Types and Time Ranges

The values for Type can be modified in the schedule window, or by selecting the item from the Doors menu, under the Schedule Manager sub-menu (Figure 9-1).

![Schedule Manager Menu](image)

The items in the Schedule Manager only define the available work weeks, holidays, time ranges, special cases and Time Entry Collections. You must still assign these values to a schedule. Once the schedule is defined, assign the schedule to an access policy, or to a door configuration. See Using the Schedule Manager, page 9-7 for more information.

- Modifying Special Cases, page 9-12
- Modifying Holidays, page 9-11
- Modifying Time Ranges, page 9-11
- Modifying Special Cases, page 9-12
- Modifying Time Entry Collections, page 9-12

Modifying Work Weeks

Work Weeks define the days of the week for a schedule.

**Step 1** Select Work Weeks from the Doors menu, under the Schedule Manager sub-menu.

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

**Step 3** Enter the name of the value and a short text description.

**Step 4** Select the days to include in the work week. For example, select Monday through Friday to define a Work week for the weekdays, or select Saturday and Sunday to define a value for the weekend.

**Step 5** Click Save and Close when you are done.
Modifying Holidays

Holiday defines a single date, or range of consecutive dates.

Step 1 Select **Holiday** from the Doors menu, under the Schedule Manager sub-menu.

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

Step 3 Enter the name and a short text description.

Step 4 To enter a **Start Date** and an **End Date** for the holiday, click each date field to open a calendar, and then double click on a date.

Step 5 For a holiday that is one day, select the same day for both the beginning and end dates.

Step 6 Click the **Today** button to reset the calendar to the current date.

Step 7 Click **Save and Close** when you are done.

---

Modifying Time Ranges

Time Ranges specify the time span for a schedule type.

Step 1 Select **Time Range** from the Doors menu, under the Schedule Manager sub-menu.

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

Step 3 In the detail window, enter the name and a short text description.

Step 4 Enter a start and end time in 24 hour format. For example, enter 13:00 for 1 p.m.

Step 5 Click **Add** to add a time range to the list **Start Time - End Time**. You can add multiple time ranges to a single entry.

Step 6 To remove a range, highlight the entry and select **Remove**.
Step 7  Click **Save and Close** when you are done.

### Modifying Special Cases

Select **Special Cases** to define a schedule for a date or range of dates that repeat on a regular schedule. For example, you can create a special case for the first Monday in each month. Select an existing Special Case from the **Value** drop-down menu, or do the following.

**Step 1**  Select **Special Cases** from the Doors menu, under the Schedule Manager sub-menu.

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

**Step 3**  Enter the name of the value and a short text description.

**Step 4**  Select the **Recurrence**. For example, **Every Year**.

**Step 5**  Select a **Day of Year** or **Month** for the recurring schedule. If you select month, select the specific month for the schedule, or select **Every Month**.

**Step 6**  Select the options for **Week** or **Day of month**.

**Step 7**  Click **Save and Close** when you are done.

### Modifying Time Entry Collections

Time Entry Collections allow you to create groups of other schedule types, including Holidays, Work Weeks, or Special Case schedules.

For example, you can define individual holidays and then group all the holidays on the calendar as a `timeEntryCollection - US Holidays Calendar`. This can then be used in a schedule entry with “Permit” or “Deny”.

**Note**  A Time Entry Collection can be used in more than one schedule, but only if the schedules have the same action (such as Allow or Deny). If a Time Entry Collection is assigned to schedules with different actions, then the schedule operation will be inconsistent.

**Step 1**  Select **Time Entry Collection** from the Doors menu, under the Schedule Manager sub-menu.
Step 2  Click **Add**, or select an existing entry and click **Edit**.

Step 3  Enter the name of the value and a short text description.

Step 4  Select the **Type**. For example, Holiday, Work Week, or Special Case.

Step 5  Select a **Value** for the selected Type. For example, if you selected the Type Holiday, select Christmas. To create a new value, click **New** to open the Add window.

Step 6  Select a **Time Range**. For example, **Default Time Range Group**. To create a new time range, click **New** to open the Add window.

Step 7  If you select month, select the specific month for the schedule, or select **Every Month**.

Step 8  Click **Add** to add the entry.

Step 9  Repeat these steps to add additional entries to the collection.

Step 10  Click **Save and Close** when you are done.
Configuring Anti-Passback Areas

Anti-passback provides a higher level of security by recording and controlling badge holder exit points as well as entry points. Anti-passback areas provide the following controls:

- Records a badge holder’s entry and exit through a door or set of doors.
- Requires that the badge holder exit through a specified door or set of doors.
- Prevents a badge holder from entering a door and then passing their badge to another person to enter the same door.

The consequences of violating the anti-passback conditions vary depending on the anti-passback mode for the access point.

To create or modify an anti-passback area, do the following:

**Step 1**
Select **Anti-Passback Areas** from the Doors menu, under the Access Policies sub-menu. The main window lists the currently defined areas, as shown in Figure 9-2.

- To modify an existing area, select the area name and choose **Edit...** to open the detail window.
- To add a new area, click **Add...** to open the detail window.
- To remove an area, highlight the area name and click **Delete**.

**Figure 9-2  Anti-Passback Area Main Window**

**Step 2**
Complete the following fields in the detail window (see Figure 9-2).

- **Name**: Enter a descriptive name for the area.
- **Anti-Passback Area Number**: Read only.
- **Comments**: Enter a description of area.
- **Site**: Read-only.
- **Anti-Passback mode**: Select one of the following modes:
  - **Hard (deny access)**: Will deny access if the badge has an incorrect entry area.
- **Soft (grant access)**: Will grant access even if the badge has an incorrect entry area, but reports the passback violation to the Cisco PAM appliance. The monitoring screen refreshes to display the new swipe-in time.

- **Timed**: The same badge cannot be used twice in a row at this access point within the time specified in the **Anti-passback delay** field. If the badge is used within the specified time, then the mode is **Hard** and access is denied. If the badge is used after the time specified, then access is granted in **Soft** mode.

f. **Anti-passback delay**: Enter the delay time, in seconds, used for the **Timed** anti-passback mode.

**Figure 9-3**  **Anti-Passback Areas Detail Window**

![Anti-Passback Areas Detail Window](image)

**Step 3**  Click **Save and Close** to save the settings and close the detail window.
Monitoring Anti-Passback Events

Use **Anti-Passback Monitoring** to view the badges that are in an anti-passback area. For example, if a user enters an anti-passback area using their badge, an entry is added to the Anti-Passback Monitoring window as shown in **Figure 9-4**. This entry remains in the list until the user exits the anti-passback area.

- To view the badges currently in any anti-passback area, select the **Anti-Passback Monitoring** module from the Doors menu, under the Access Policies sub-menu. **Figure 9-4** shows the main window.
- To reset the state of a badge, select an entry and click the **Reset** button.

**Figure 9-4  Anti-Passback Monitoring Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Name</td>
<td>The anti-passback area accessed by the badge. See Configuring Anti-Passback Areas, page 9-14 for more information.</td>
</tr>
<tr>
<td>Badge ID</td>
<td>The ID number of the badge.</td>
</tr>
<tr>
<td>Door Name</td>
<td>The name of the door accessed.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the Anti-Passback area. See Configuring Anti-Passback Areas, page 9-14 for more information.</td>
</tr>
<tr>
<td>Swipe In Time</td>
<td>The day and time when the entry door was accessed.</td>
</tr>
<tr>
<td>Facility Code</td>
<td>The facility code.</td>
</tr>
</tbody>
</table>

**Anti-Passback Events Displayed in the Events Module**

An event is also generated whenever a badge holder swipes a badge in an anti-passback area. These events are displayed in the Events module, as described in **Viewing Events**, page 10-3.

For example, if a badge is swiped at a door configured with the anti-passback mode **Hard (deny access)**, an event is generated such as “Badge is not Authorized due to Hard Anti-Passback policy”. A badge swiped at a door with the mode **Soft (grant access)** generates an event “Badge is Authorized”. 
Configuring Two-Door Policies

A two-door policy requires that when a user accesses a door, they must also access a second door in a set number of seconds.

To configure two-door policies, do the following:

**Step 1**
Select **Two-Door Policy** from the Doors menu, under the Access Policies sub-menu. The main window is shown (see Figure 9-5).

- To modify an existing policy, select the entry and choose **Edit...** to open the detail window. You can also double-click the entry.
- To add a new policy, click **Add...** to open the detail window.
- To remove an policy, highlight the entry and click **Delete**.

![Figure 9-5 Two-Door Policy Main Window](image)

**Step 2**
Complete the fields in the detail window, as shown in the following Figure 9-6:

![Figure 9-6 Two-Door Policy Detail Window](image)

- **Name**: Enter a short description of the policy. For example: *Building 1 lab doors*.
- **Door 1**: Click **Select Door 1** to open the pop-up window (Figure 9-7). Select a door from the list and click **OK**. The door should include an exit reader in addition to an entry reader. Use the search field at the top of the window to narrow the list of doors, if necessary.
- **Door 2**: Click **Select Door 2** to open the pop-up window. Select a door from the list and click **OK**. Use the search field at the top of the window to narrow the list of doors, if necessary. Door 2 does not require an exit reader.
- **Time Interval (sec)**: Enter the maximum time, in seconds, that a user is allowed between accessing the first door and the accessing the second door.
- **Enabled**: Check the enabled box to enable the policy.

**Figure 9-7  Select Door 1 Window**

Step 3  Click **Save and Close** to save the changes and close the detail window.
**Two-Door State Monitoring**

Use the **Two-Door State Monitoring** module to display events for doors configured with the **Two-Door Policy** module.

**Step 1**
Select **Two-Door State Monitoring** from the Doors menu, under the Access Policies sub-menu. The main window is shown (see Figure 9-8).

**Step 2**
To display details for the event, highlight an entry and click **Edit**....

**Figure 9-8 Two-Door State Monitoring Main Window**

An two-door state event has the properties described below, available in the table view or detail window:

<table>
<thead>
<tr>
<th><strong>Table 9-2 Two-Door State Monitoring Properties</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Badge ID</td>
</tr>
<tr>
<td>Door Name</td>
</tr>
<tr>
<td>Policy Name</td>
</tr>
<tr>
<td>Swipe In Time</td>
</tr>
<tr>
<td>Facility Code</td>
</tr>
</tbody>
</table>

**Step 3**
Click **Close** to close the detail window.
CHAPTER 10

Events & Alarms

This chapter describes how to view events and alarms in Cisco PAM. It also includes instructions to configure the event policies that define how events are captured and managed.

Events can be viewed in the following ways:

- As a list using the Events or Alarms modules.
- Using an audit trail of events initiated by a user.
- By personnel photos.
- Using graphic maps to display where events occur on a floor or building. You can also use the map to trigger actions for a device or door.

Tip

To create actions that are triggered by an event, see Chapter 11, “Configuring Automated Tasks”.

To view live and recorded video for events and alarms, see Chapter 13, “Video Monitoring”.

Contents

- Viewing Events, Alarms and Audit Trail Records, page 10-3
  - Viewing Events, page 10-3
  - Viewing Alarms, page 10-8
  - Viewing Audit Trail Records, page 10-13
  - Viewing Recent Events for a Device, Driver, or Location, page 10-16
- Viewing Events Using Personnel Photos, page 10-17
  - Viewing Event Photos, page 10-17
  - Adding a Color Border to Event Photos (Credential Watch), page 10-18
  - Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 10-21
- Recording External Events, page 10-25
- Viewing Workstation Activity, page 10-27
- Configuring Events and Alarms, page 10-28
  - Modifying Default Event Policies, page 10-28
  - Automatically Open the Alarm Window, page 10-33
• Configuring Time Schedules, page 10-34
• Configuring Alert Sounds, page 10-36
• Setting Event and Alarm Priorities, page 10-37
• Defining User Privileges for Editing Events, page 10-38

• Using Graphic Maps, page 10-39
  – Graphic Maps Viewer, page 10-39
  – Graphic Map Editor, page 10-42

• Archiving Historical Events, page 10-47
  – Using Driver Commands to Copy and Prune Historical Events, page 10-48
  – Creating an Automated Rule to Archive Historical Events, page 10-51
  – Creating Reports from the Historical Events Archive, page 10-55
Viewing Events, Alarms and Audit Trail Records

Events and alarms are captured in real time, and are accessed in the **Events & Alarms** menu, under the **Monitoring** sub-menu. The Events window includes all events in the system. Alarms are critical or important events. Audit trails are events initiated by users.

This section includes the following:

- Viewing Events, page 10-3
- Viewing Alarms, page 10-8
  - Alarm States, page 10-9
  - Alarm Detail Window, page 10-9
- Viewing Audit Trail Records, page 10-13

**Tip**

See Configuring Events and Alarms, page 10-28 to define or modify event types. To copy or move events to a historical events archive, see Archiving Historical Events, page 10-47.

Viewing Events

You can view events in a list, or double-click an event to view detailed information. You can also right-click an event to select commands, change the event properties, or view associated video.

**Step 1**

Select **Events** from the Events & Alarms menu, under the Monitoring sub-menu. The Events window (Figure 10-1) shows the most recent events in the access-control system.

![Figure 10-1 Events Module Main Window](image)
**Step 2**  Modify the list of records using the following toolbar controls:

- **Scroll Lock**: Disables or enables automatic scrolling of the list as new events are inserted.
- **Clear List**: Clears all events from the table. Only new events are displayed.
- **View...**: Select an event and click View to display the detail window (Figure 10-2). You can also double-click the event.
- **Report...**: View the selected events in a separate window, or save the information in a file. See Creating Reports, page 3-10.
- **Columns...**: Define the columns displayed and their order. See Revising the Column Display, page 3-14.
- **Filter**: Filter the events to display a sub-set of records. To change the number of viewable events, select **Max rows**. See Using Filters, page 3-12.
- **Search**: See Search, page 3-15.

**Step 3**  Select a record and click **View...** to open the detail window (Figure 10-2). You can also double-click the record.

*Figure 10-2  Events Module Detail Window*
Step 4 Review the properties and actions for the record. See Table 10-1 for field descriptions.

Note Event fields available vary depending on the type of event. The following example is for a door event.
### Table 10-1  Event Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time and date when the event occurred.</td>
</tr>
<tr>
<td>Time received</td>
<td>The time the event was received and stored in the database. If the event was processed by an external device such as a Gateway, this may differ from the time, depending on delays or interruptions in communications between the host and the device.</td>
</tr>
<tr>
<td>Site</td>
<td>A site is a single instance of a Cisco PAM database.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of event. The types of events are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Event:</strong> A general occurrence within the system, often from external hardware such as a Gateway.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alarm:</strong> An event configured to be an alarm.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alarm Annotation:</strong> An event caused by commenting, clearing, or acknowledging alarms.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Audit Record:</strong> An event caused by an operator modifying a record, such as a badge or personnel record.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device Command:</strong> An event caused by an operator executing a device command.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device Command Result:</strong> Notification of a completed device command.</td>
</tr>
<tr>
<td>Log Code</td>
<td>The internal code to identify the event. Log codes can be viewed in the Event Policy Manager and defined as alarms. See Modifying Default Event Policies, page 10-28.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the event.</td>
</tr>
<tr>
<td>Priority</td>
<td>The importance level assigned to the event. Priorities range from a low of -10 to a high of 10. To configure these priorities, see Setting Event and Alarm Priorities, page 10-37.</td>
</tr>
<tr>
<td>Device</td>
<td>The device associated with the event, such as a workstation or hardware module.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit...:</strong> Displays information about the device including type, name, and address. Some fields are editable, depending on the type of device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View Status...:</strong> Displays the status of the associated device. For example, if the workstation is logged in to the system or if the hardware module is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Commands:</strong> lists any available commands for the device. For example, apply a Gateway configuration, or send a message to a workstation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Show in Graphics Map:</strong> see Graphic Maps Viewer, page 10-39.</td>
</tr>
<tr>
<td>Credential</td>
<td>If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit...:</strong> Revise the credential (badge, login, etc.) record associated with the event.</td>
</tr>
<tr>
<td>Watch Level</td>
<td>Displays the Credential Watch Level for the badge associated with the event. See Adding a Color Border to Event Photos (Credential Watch), page 10-18.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit...:</strong> Revise the credential watch level associated with the badge.</td>
</tr>
</tbody>
</table>
Table 10-1  Event Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel Record</td>
<td>If a personnel record is associated with the event, this field displays the person’s name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit...</strong>: Edit the personnel record associated with the event.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View Photo...</strong>: Displays the associated personnel record photo, if any.</td>
</tr>
<tr>
<td>Data</td>
<td>This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.</td>
</tr>
<tr>
<td>Target device</td>
<td>The device associated with the event. For example, the device where a command was executed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong>: modify the device settings.</td>
</tr>
<tr>
<td>camera</td>
<td>The camera associated with the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Live Video</strong>: opens the video player to view live video from the camera associated with the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Event Video</strong>: displays archived video associated with the event, if available.</td>
</tr>
</tbody>
</table>

See Chapter 13, “Video Monitoring” for more information.
Viewing Alarms

Alarms are a type of event that indicate the event is important or requires additional attention. You can acknowledge, clear, and add comments to an alarm.

- In other modules, an alarm summary is displayed in the lower left-hand corner of the window.
- For instructions to open Alarms when an alarm occurs, see Automatically Open the Alarm Window, page 10-33.

This section includes the following:
- Main Alarm Window, page 10-8
- Alarm States, page 10-9
- Alarm Detail Window, page 10-9
- Alarm Properties, page 10-10

Main Alarm Window

To view alarms, do the following

**Step 1** Select **Alarms** from the **Events & Alarms** menu, in the **Monitoring** menu. The main window (Figure 10-3) shows the most recent 500 uncleared alarms.

*Figure 10-3  Alarms Module Main Window*

- **Step 2** Modify the list of records using the following toolbar controls:
  - **Scroll Lock**: Disables or enables automatic scrolling of the list as new events are inserted.
  - **Report...**: View the selected alarms in a separate window, or save the information in a file. See Creating Reports, page 3-10.
  - **Columns...**: Define the columns displayed and their order. See Revising the Column Display, page 3-14.
• **Filter**: Filter the alarms to display a sub-set of records. To change the number of displayed alarms, select **Max rows**. See Using Filters, page 3-12.

**Step 3**

Change the state of an alarm, add a comment, or acknowledge the alarm.

Use the following toolbar buttons or right-click the entry and select an option from the menu.

- **Ack**: Acknowledges an alarm, placing it in an acknowledged state. This means that the operator is aware of the alarm, but it has not been resolved. A solid orange color indicates this state.
- **Comment**: Adds a comment to an alarm. Does not change the state of the alarm. A new comment may be entered, or a previously entered comment may be selected from the drop-down list.
- **Clear**: Places the alarm in a cleared state (resolved) and changes the icon to green.

See Alarm States for more information. The alarms state options are also available in the detail window.

**Step 4**

Select an alarm and click **View**... to open the detail window (Figure 10-4 on page 10-10). You can also double-click the record. See Alarm Properties, page 10-10 for field descriptions.

---

### Alarm States

An alarm may be in one of several states, and these states have an associated solid or blinking color.

**Table 10-2  Alarm States**

<table>
<thead>
<tr>
<th>State</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Blinking red</td>
<td>The alarm is new, unacknowledged, and unresolved.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Solid orange</td>
<td>An operator is aware of the alarm, though it remains unresolved.</td>
</tr>
<tr>
<td>Cleared</td>
<td>Solid green</td>
<td>The alarm has been acknowledged and resolved. Note that the default filter in the Alarms module hides cleared alarms, so these are generally not seen.</td>
</tr>
</tbody>
</table>

### Alarm Detail Window

The detail window (Figure 10-4) displays alarm properties and provides a number of actions:

- The Alarms tab displays the properties of the alarm and provides a number of actions. See Alarm Properties, page 10-10 for more information.
- The Duplicates tab displays duplicate alarms. All attributes are the same except the time.
- The Annotations tab displays any annotations made to the selected alarm. Valid alarm annotations include:
  - Acknowledge Alarm
  - Clear Alarm
  - Comment Alarm
Alarm Properties

An alarm has the following properties, available in the table view or the detail window:

Table 10-3    Alarm Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The date and time when the alarm occurred.</td>
</tr>
<tr>
<td>Time Received</td>
<td>The time the alarm was received and stored in the database. If the event was processed by an external device such as a Gateway, this may differ from the time, depending on delays or interruptions in communications between the host and the device.</td>
</tr>
<tr>
<td>Site</td>
<td>The site where the alarm occurred.</td>
</tr>
<tr>
<td>Log Code</td>
<td>The internal code to identify the event. Log codes can be viewed in the Event Policy Manager and defined as alarms. See Modifying Default Event Policies, page 10-28.</td>
</tr>
<tr>
<td>Priority</td>
<td>The level of importance assigned to the alarm. Priorities range from a low of -10 to a high of 10. To configure these priorities, see Setting Event and Alarm Priorities, page 10-37.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the alarm.</td>
</tr>
</tbody>
</table>
### Table 10-3 Alarm Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td>The device associated with the alarm, such as a workstation or hardware module.</td>
</tr>
<tr>
<td></td>
<td>- <em>Edit...</em>: Displays information about the device including type, name, and address. Some fields are editable, depending on the type of device.</td>
</tr>
<tr>
<td></td>
<td>- <em>View Status...</em>: Displays the status of the associated device. For example, if the workstation is logged in to the system or if the hardware module is enabled.</td>
</tr>
<tr>
<td></td>
<td>- <em>Commands</em>: lists any available commands for the device. For example, apply a Gateway configuration, or send a message to a workstation.</td>
</tr>
<tr>
<td><strong>Credential</strong></td>
<td>If the alarm has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.</td>
</tr>
<tr>
<td></td>
<td>- <em>Edit...</em>: Revise the credential (badge, login, etc.) record associated with the event.</td>
</tr>
<tr>
<td><strong>Watch Level</strong></td>
<td>Displays the Credential Watch Level for the badge associated with the event. See Adding a Color Border to Event Photos (Credential Watch), page 10-18.</td>
</tr>
<tr>
<td></td>
<td>- <em>Edit...</em>: Revise the credential watch level associated with the badge.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>The address of the device.</td>
</tr>
<tr>
<td><strong>Personnel Record</strong></td>
<td>If a personnel record is associated with the alarm, this field displays the person’s name.</td>
</tr>
<tr>
<td></td>
<td>- <em>Edit...</em>: Edit the personnel record associated with the event.</td>
</tr>
<tr>
<td></td>
<td>- <em>View Photo...</em>: Displays the associated personnel record photo, if any.</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, this field contains the card number.</td>
</tr>
<tr>
<td><strong>Count</strong></td>
<td>The number of times this alarm has occurred, including duplicates. Duplicate alarms have all attributes the same except time).</td>
</tr>
<tr>
<td><strong>Alarm State</strong></td>
<td>The state of the alarm. See Alarm States, page 10-9.</td>
</tr>
<tr>
<td></td>
<td>- <em>Ack...</em>: Acknowledges the alarm, placing it in an acknowledged state. This means that the operator is aware of the alarm, but it has not been resolved. A solid orange color indicates this state.</td>
</tr>
<tr>
<td></td>
<td>- <em>Clear...</em>: Clears the alarm, placing it in a cleared state. This means that the alarm has been resolved. A solid green color indicates this state.</td>
</tr>
<tr>
<td></td>
<td>- <em>Comment...</em>: Adds a comment to an alarm. Does not change the state of the alarm. A new comment may be entered, or a previously entered comment may be selected from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>- <em>View Instructions...</em>: Opens a detail window with instructions for dealing with the type of alarm, if any.</td>
</tr>
</tbody>
</table>
**Table 10-3 | Alarm Properties (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Target device | The device associated with the event. For example, the device where a command was executed.  
   - **Edit**: modify the device settings.  
| camera    | The camera associated with the device.  
   - **Live Video**: opens the video player to view live video from the camera associated with the device.  
   - **Event Video**: displays archived video associated with the event, if available.  

See Chapter 13, “Video Monitoring” for more information.
Viewing Audit Trail Records

Audit trail records are events caused when an operator modifies a record, such as a badge or personnel record. Audit trail records include the user who performed the action, the date, time, and the state of the object before and after the edit. To view audit trail records, do the following:

**Step 1** Select Audit Trail from the Reports menu. The main window (Figure 10-5) shows the most recent audit records.

**Figure 10-5  Audit Trail Main Window**

Step 2 Modify the list of records using the following toolbar controls:

- **Scroll Lock**: Disable or enable automatic scrolling of the list as new audit records are inserted.
- **Columns...**: See Revising the Column Display, page 3-14.
- **Filter**: See Using Filters, page 3-12.

Step 3 Select a record and click View... to open the detail window (Figure 10-6). You can also double-click the record.

Step 4 Review the properties and actions for the record. See Table 10-4 for field descriptions.
Figure 10-6  Audit Trail Detail Window

Table 10-4  Audit Trail Event Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time received</td>
<td>The time the event was received and stored in the database. If the event was processed by an external device such as a Gateway, this may differ from the time, depending on delays or interruptions in communications between the host and the device.</td>
</tr>
<tr>
<td>Site</td>
<td>A site is a single instance of a Cisco PAM database.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of event. The types of events are:</td>
</tr>
<tr>
<td></td>
<td>- Event: A general occurrence within the system, often from external hardware such as a Gateway.</td>
</tr>
<tr>
<td></td>
<td>- Alarm: An event configured to be an alarm.</td>
</tr>
<tr>
<td></td>
<td>- Alarm Annotation: An event caused by commenting, clearing, or acknowledging alarms.</td>
</tr>
<tr>
<td></td>
<td>- Audit Record: An event caused by an operator modifying a record, such as a badge or personnel record.</td>
</tr>
<tr>
<td></td>
<td>- Device Command: An event caused by an operator executing a device command.</td>
</tr>
<tr>
<td></td>
<td>- Device Command Result: Notification of a completed device command.</td>
</tr>
<tr>
<td>Log Code</td>
<td>The internal code to identify the event. Log codes can be viewed in the Event Policy Manager and defined as alarms. See Modifying Default Event Policies, page 10-28.</td>
</tr>
<tr>
<td>Priority</td>
<td>The importance level assigned to the event. Priorities range from a low of -10 to a high of 10. To configure these priorities, see Setting Event and Alarm Priorities, page 10-37.</td>
</tr>
</tbody>
</table>
Table 10-4  Audit Trail Event Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the event.</td>
</tr>
<tr>
<td>Device</td>
<td>The device associated with the event, such as a workstation or hardware module.</td>
</tr>
<tr>
<td></td>
<td>• Edit...: Displays information about the device including type, name, and address. Some fields are editable, depending on the type of device.</td>
</tr>
<tr>
<td></td>
<td>• View Status...: Displays the status of the associated device. For example, if the workstation is logged in to the system or if the hardware module is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Commands: lists any available commands for the device. For example, apply a Gateway configuration, or send a message to a workstation.</td>
</tr>
<tr>
<td></td>
<td>• Show in Graphics Map: see Graphic Maps Viewer, page 10-39.</td>
</tr>
<tr>
<td>Credential</td>
<td>If the event has an associated credential (such as a badge or login), the identifying information of the credential (such as a card or username) is displayed in this field.</td>
</tr>
<tr>
<td></td>
<td>• Edit...: Revise the credential (badge, login, etc.) record associated with the event.</td>
</tr>
<tr>
<td>Watch Level</td>
<td>Displays the Credential Watch Level for the badge associated with the event. See Adding a Color Border to Event Photos (Credential Watch), page 10-18.</td>
</tr>
<tr>
<td></td>
<td>• Edit...: Revise the credential watch level associated with the badge.</td>
</tr>
<tr>
<td>Personnel Record</td>
<td>If a personnel record is associated with the event, this field displays the person’s name.</td>
</tr>
<tr>
<td></td>
<td>• Edit...: Edit the personnel record associated with the event.</td>
</tr>
<tr>
<td></td>
<td>• View Photo...: Displays the associated personnel record photo, if any.</td>
</tr>
<tr>
<td>Data</td>
<td>This field displays detailed information about the event, the exact value and meaning of which depends on the type of event. This field is generally for advanced or troubleshooting use. If the event is associated with an attempt to gain access to an access point using a badge that is not in the database, then this field contains the card number.</td>
</tr>
<tr>
<td>Modified Record</td>
<td>The item changed by the user.</td>
</tr>
<tr>
<td></td>
<td>• View Current...: Opens a detail window of the modified record, as it exists currently.</td>
</tr>
<tr>
<td></td>
<td>• View Before...: Opens a detail window of the modified record, as it existed before the modification.</td>
</tr>
<tr>
<td></td>
<td>• View After...: Opens a detail window of the modified record, as it existed after the modification.</td>
</tr>
</tbody>
</table>
Viewing 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 10-7.

**Figure 10-7 View Recent Events Menu**

**Step 4** Double-click an event to view event details, as shown in Figure 10-8.

**Figure 10-8 Recent Events**
Viewing Events Using Personnel Photos

Use the Event Photos module to display events using personnel photos.

This section includes the following:

- Viewing Event Photos, page 10-17
- Adding a Color Border to Event Photos (Credential Watch), page 10-18
- Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 10-21

Viewing Event Photos

Event Photos displays events along with a personnel photo and other information in real-time.

**Step 1** Select Event Photos in the Events & Alarms menu, in the Monitoring sub-menu.

**Step 2** Select a photo to display the associated event (Figure 10-9).

**Figure 10-9  Event Photos Window**

- **Step 3** From the main window, you can perform the following actions:
  - **Filter:** Filter to display specific types of events (see Using Filters, page 3-12 and Using Filters to Limit the Photos and Doors Events Displayed by Event Photos, page 10-21).
  - **View:** Select the type of display preferred for viewing event photos. Options include:
    - **Scroll Photos From:** In a left to right layout the most recent event is displayed at the right of the screen. The opposite is true for right to left.
    - **Show Event Detail Buttons:** Displays the buttons in the detail area.

Note: The screen appears blank (without fields or data) until a photo event is available for display.
- **Max Photos**: Defines the number of most recent photos to display in the window.
  - **Resume**: Resume the scrolling of new events.
  - **Pause**: Pause the scrolling of new events.

**Tip**
See Viewing Events, Alarms and Audit Trail Records, page 10-3 for field descriptions. To make the event fields read-only, see Configuring Events and Alarms, page 10-28.

### Adding a Color Border to Event Photos (Credential Watch)

Credential watch allows you to display event photos with a colored border to provide additional information regarding the status of the badge holder.

For example, if a guard uses Event Photos to view photos of the people accessing a door, a colored border can visually signify if the user is a contractor, visitor, etc..

The default credential watch levels are:
- **Low**: a yellow border around the photo.
- **Medium**: an orange border around the photo.
- **High**: a red border around the photo.

You can modify these definitions, or create custom watch levels. For example, if the badge holder has been employed less than one year, an ORANGE border may appear around the photo. If the badge holder is a contractor, a RED border may appear around the photo.

To configure Credential Watch, do the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Enable Credential Watch Levels menu:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Select <strong>System Configuration</strong> from the Admin menu.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Select the <strong>Miscellaneous</strong> tab.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Select the <strong>Enable credential watch levels</strong> check-box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Click <strong>Save</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Log out and log back in to Cisco PAM to activate the changes (select <strong>Log Out</strong> from the Options menu).</td>
<td></td>
</tr>
</tbody>
</table>
To do this | Use this display
---|---
**Step 2** Add credential watch access privileges for user profiles:  
a. Select **Profiles** from the Users menu.  
b. Click **Add** or select an existing profile and click **Edit**.  
c. Click the **Module** tab.  
d. Click **Quick Launch**.  
e. Select the options in the panel to the right.  
f. Click **Save and Close**.  

**Tip** For more information, see Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client”.

(Optional) Assign the profile to the user login, if necessary:  
a. Select **Login** from the Users menu.  
b. Click **Add** or select an existing user and click **Edit**.  
c. Select **Profiles**.  
d. Select the profile that includes the required access privileges.  
e. Click **Save and Close**.
### Step 3
(Optional) Create or edit the credential watch definitions.

**Tip** This defines the photo border color and description:

- a. Select **Credential Watch Levels** from the Admin module.
- b. Click **Add** or select an existing level and click **Edit**.
- c. Enter the **Name** of the level. For example: New Employee.
- d. Enter the order number of the level to define the hierarchy of the levels. For example, enter 0 to display the new level at the top of the list. This can also define the relative importance or severity of the levels.
- e. Click **Choose** to select a border color for the photos when using **Event Photos**.
- f. Click **Save and Close**.

### Step 4
Add the credential watch level to a badge configuration:

- a. Select **Badges** from the Admin module.
- b. Click **Add** or select an existing badge and click **Edit**.
- c. Select the **General** tab.
- d. Select the Watch Level from the drop-down menu. For example, **New Employee**.

### Step 5
Open the **Event Photos** module: select **Event Photos** from the Events & Alarms menu, in the Monitoring sub-menu.
Viewing Events Using Personnel Photos

Using Filters to Limit the Photos and Doors Events Displayed by Event Photos

By default, Event Photos displays the photos and events for any badge presented to any door on the system. Use the Filter to display only events for a specific door or set of doors. For example, the guard at the front entrance should only see the event photos for badges presented at that particular door.

In addition, the photo associated with a badge is shown two times by default: one time when the credential is read, and one time for the Grant Access event. Use Filters to only display the photo once.

Complete the following instructions to limit the doors and photos displayed by Event Photos:

**Step 1** To select specific doors to display event information:

a. Select **Edit Filter** from the Filters toolbar menu.

b. In the filter window, select the **Device** tab, and then select the **Choose** button (Figure 10-10).

c. Select the doors or devices that will display events in Event Photos.

d. Click **OK** to close the Choose Devices window.

e. Click **OK** to close the Filter window and save the changes.

Note: The screen appears blank (without fields or data) until a photo event is available for display.
Step 2  To display the photo once for each badge presentation:

a. In the filter window, select the General tab, and then select the Choose button in the Log Code field (Figure 10-11).
**Figure 10-11  Filter Log Code**

![Filter Log Code](image-url)
b. Select the events to be displayed in Event Photos, as shown in Figure 10-12. For example, select Door Grant Access.

Figure 10-12    Select the Log Code

![Choose Log Codes window]

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

   c. Click OK to close the windows and save the changes.
Recording External Events

External applications can record events in Cisco PAM using the `recordExtEvent` API. Once recorded, the events are displayed in the Events & Alarms Monitoring modules.

External Event Types are defined using the Event Definition Format and imported using the steps described in the following sections.

To record events from external applications, do the following:

1. **Define External Event Types Using the Event Definition Format, page 10-25.** This file also defines the categories for the log codes.
2. **Create a Text File to Define the Event Names in Cisco PAM, page 10-26.**
3. **Import the Files into Cisco PAM, page 10-26.**
4. **Add external events and alarms to Cisco PAM using the `recordExtEvent` API, as described in the Cisco Physical Access Control API Reference Guide.**

Define External Event Types Using the Event Definition Format

Use the Event Definition Format to create an XML file that defines the event and alarm codes used to add external events to Cisco PAM. This file also defines the category for the events and is imported into Cisco PAM to create the codes.

**Example**

In the following XML example:

- The concatenation rule is: `AE.<logcode_prefix>_<logcode>`
- Event category: `AE.Cisco_VSM`
- The log codes for the category are: `AE.VS_VSM_Sample1` and `AE.VS_VSM_Sample2`

```xml
<appext_eventdefns
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <appext_entry appname="Cisco_VSM" logcode_prefix="VS">
      <ext_event_defn logcode="VSM_Sample1" priority="10" description="VSM Sample Event-1"/>
      <ext_event_defn logcode="VSM_Sample2" priority="10" description="VSM Sample Event-2" isAlarm="true"/>
   </appext_entry>
</appext_eventdefns>
```

The file is saved with the `.xml` extension. For example: `SampleExtEventDefs.xml`. 

Create a Text File to Define the Event Names in Cisco PAM

To define the log code names displayed in Cisco PAM, create a text file that defines a string name for each event and the event category.

In the following example, the string name for the two events and the event category are defined:

VS_VSM_Sample1=Sample Event-1
VS_VSM_Sample2=Sample Event-2
Cisco_VSM=Cisco Video Surveillance Manager

The file is saved with the .properties extension. For example: AppExtMessages.properties.

Import the Files into Cisco PAM

Once the XML and properties files are created, import the files into the Cisco PAM External Events module.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>External Events</strong> from the Events &amp; Alarms menu.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Import</strong>.</td>
</tr>
</tbody>
</table>
| **Step 3** | a. Select the XML and Properties files.  
   • The XML file defines the event log codes and category for the external events.  
   • The Properties file defines the text string for each code and category. The text string is the name that appears in Cisco PAM.  
   b. Click **Next** to preview the settings, or click **Finish** to save the changes.  

For instructions to create these files, see:  
• Define External Event Types Using the Event Definition Format, page 10-25  
• Create a Text File to Define the Event Names in Cisco PAM, page 10-26 |
To view a summary of the users who access the system, select Workstations from the Events & Alarms menu, under the Monitoring sub-menu. The Workstations window (Figure 10-13) shows the most recent events in the access-control system.

**Figure 10-13  Workstations Main Window**

To view additional details, such as the credentials and connected time, double click a user name.
Configuring Events and Alarms

This section includes instructions to customize the behaviour of system events. For example, you can treat an event as an alarm, suppress recording, set the event priority, define the sound played for an alarm, and other settings.

**Tip**
To automatically trigger actions when an event occurs, see Chapter 11, “Configuring Automated Tasks”.

**Contents**

- Modifying Default Event Policies, page 10-28
- Automatically Open the Alarm Window, page 10-33
- Configuring Alert Sounds, page 10-36
- Setting Event and Alarm Priorities, page 10-37
- Defining User Privileges for Editing Events, page 10-38

**Note**
Event policies are executed only on the Cisco PAM server.

This section also includes instructions to limit the type of events seen by users, and configure the Alarms module to automatically open when an alarm occurs.

**Modifying Default Event Policies**

Each event or alarm record includes a log code that defines the event type and actions associated with the event. The built-in event policies define inherent system behavior, such as which events are also alarms, and which events are recorded to the database (all built-in events are recorded to the database by default). These built-in policies are based on the log code only: no other criteria are used to define the event trigger.

The default event policies should be changed only if you need to change an inherent event behavior. For example:

- Whether the event is an alarm or an event.
- Whether the event is saved to the database.
- The event priority.
- The sound played when the event is triggered.
- The color shown for the event in the event modules.

When custom events are required, we recommend creating a custom event policy, as described in the following section.

**Configuring Custom Event Policies**

Event policies can be configured to trigger events and alarms based on one or more conditions, such as the event type, the source device, device type, location, time of occurrence, or other factors.
• If an event policy includes more than one condition, all the conditions must match for the event to be triggered.

• If multiple events apply to an event occurrence, the most specific event policy is executed. Since only one event policy can be triggered for any event, only the most specific event is used. To determine the most specific event, the following criteria are applied in decreasing order (the criteria at the top of the list are given greater importance):

1. Log code
2. Log code category
3. Device instance
4. Device group
5. Partition
6. Hierarchical location (Building, Area, etc.)
7. Device type
8. Time schedule
9. Invert time schedule (That is, “Not in” time schedule)

Examples

• If one event policy is based on a log code (such as Door Forced Open) and a second event policy uses the same log code in combination with other criteria (such as Time schedule), then the second event policy is selected.

• If one event policy is based on a device type, and a second is based on a device instance, then the device instance event prevails since it is higher in the list of criteria.

• If two event policies are based on the same time schedule, but the first event defines During time schedule and the second event defines Not during time schedule, the first one event policy is used since During time schedule is higher in the list.

• If one event policy is based on a log code and a second policy is based on a collection of log codes and a location, all events in that location will use the second policy. Events from other locations will use the first policy.
To modify event policies, do the following:

**Step 1** Select **Event Policy Manager** from the **Events & Alarms** menu, in the **Configuration** sub-menu.

**Step 2** The main window (Figure 10-14) shows all event policies defined within the system.

*Figure 10-14  Event Policy Manager Module Main Window*

**Step 3** Modify the events, if necessary:
- Select an existing entry and click **Edit**. The detail window opens, as shown in Figure 10-15. You can also double-click the entry.
- Click **Add...** to open the detail window (Figure 10-15) and add a new event policy.
- Select an entry and click **Delete** to delete the selected event policy.

Each field is described in Table 10-5 on page 10-31.
Event Policy Properties

An event policy has the following properties:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Code</td>
<td>An abbreviated code uniquely identifying the event.</td>
</tr>
<tr>
<td>Log code description</td>
<td>The description associated with the log code.</td>
</tr>
<tr>
<td>Applies To</td>
<td>The type of event this log code applies to.</td>
</tr>
<tr>
<td>Log code category</td>
<td>The category associated with the log code.</td>
</tr>
</tbody>
</table>
## Event Policy Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device</strong></td>
<td>If specified, the policy only applies to the device. Click <strong>Choose</strong> to select the device. Click <strong>Clear</strong> to remove the device. If no device is specified, the event applies to all devices.</td>
</tr>
<tr>
<td><strong>Device Group</strong></td>
<td>If specified, the policy only applies to the device group (for example: Door, Gateway, or Reader). Click <strong>Choose</strong> to select the group. Click <strong>Clear</strong> to remove the group. If no device group is specified, the event applies to all device groups. See also Configuring Device Groups, page 6-28.</td>
</tr>
<tr>
<td><strong>Partition</strong></td>
<td>If present, the policy only applies to this partition.</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>If present, the policy only applies to this classification.</td>
</tr>
<tr>
<td><strong>Anti-passback area</strong></td>
<td>If present, the policy only applies to this anti-passback area.</td>
</tr>
<tr>
<td><strong>Anti-passback area (exit)</strong></td>
<td>If present, the policy only applies to this anti-passback area exit.</td>
</tr>
<tr>
<td><strong>Entrance</strong></td>
<td>If present, the policy only applies to this entrance.</td>
</tr>
<tr>
<td><strong>Zone</strong></td>
<td>If present, the policy only applies to this zone.</td>
</tr>
<tr>
<td><strong>Hierarchical location</strong></td>
<td>If present, the policy only applies to the doors in this location.</td>
</tr>
<tr>
<td><strong>Device type</strong></td>
<td>If present, the policy only applies to devices of this type.</td>
</tr>
<tr>
<td><strong>Time Schedule</strong></td>
<td><strong>Any time</strong> Generate events at all times and dates.</td>
</tr>
<tr>
<td></td>
<td><strong>During time schedule</strong> Generate events only during the specified <strong>Time schedule</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Not during time schedule</strong> Do not generate events during the specified <strong>Time schedule</strong>. Generate events at all times outside the specified <strong>Time schedule</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Time schedule</strong> Specifies the time schedule used for event policies. See Configuring Time Schedules, page 10-34 for more information.</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td><strong>Is Alarm</strong> Specifies if events with this log code will be recorded as an alarm. Alarms are shown in the <strong>Alarms</strong> module.</td>
</tr>
<tr>
<td></td>
<td><strong>Is Recorded</strong> Specifies if events with this log code will be recorded to the database. If unchecked, there is no record of these events occurring. This should only be unchecked by advanced users under the advice of Cisco technical support.</td>
</tr>
<tr>
<td></td>
<td><strong>Priority</strong> A priority used for sorting events and alarms. Positive priorities are above normal priority, while negative priorities are below normal priority. Zero is normal.</td>
</tr>
<tr>
<td></td>
<td><strong>Alert Sound</strong> The sound to be played, if <strong>Is Alarm</strong> is checked. Available alert sounds are managed in Configuring Alert Sounds, page 10-36. Click <strong>Play</strong> to preview the alarm sound.</td>
</tr>
<tr>
<td></td>
<td><strong>Background color</strong> The color of the event entry. Click <strong>Choose</strong> to select a color. Click <strong>Clear</strong> to restore the default white background.</td>
</tr>
<tr>
<td></td>
<td><strong>Foreground color</strong> The color of the event text. Click <strong>Choose</strong> to select a color. Click <strong>Clear</strong> to restore the default black text.</td>
</tr>
</tbody>
</table>
Automatically Open the Alarm Window

To automatically open the alarm window when an alarm occurs, do the following:

Step 1  Select Profiles from the Users menu.
Step 2  Click Add, or select an existing profile and click Edit.
Step 3  Select the General tab, and the sub-menu Events/Alarms (Figure 10-16).
Step 4  Select the check-box for Open Alarms Module.
Step 5  Click Save and Close.

Tip  Be sure that the user has access to the Alarms module. Click the Modules tab, select Alarms from the module list, and select the check box for Allow access to module. For more information, see Defining User Profiles for Desktop Application Access, page 4-2.

Figure 10-16  Profile: General Tab
Configuring Time Schedules

Time schedules define when events and automated rules will run. See Configuring Events and Alarms, page 10-28 and Configuring Global I/O Automated Rules, page 11-12 for more information.

To create and modify time schedules, do the following:

**Step 1** Select **Time Schedules** from the Admin menu.

The main window displays the currently defined time schedules, as shown in Figure 10-17.

*Figure 10-17  Time Schedule: Main Window*

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

You can also right-click an entry and select **Add**, **Edit**, or **Delete**.

**Step 3** (Add or Edit only) Enter a name for the schedule, as shown in Figure 10-18.

*Figure 10-18  Time Schedule: Detail Window*
Step 4  Select a **Priority**.

Step 5  Define the schedule times:
   a. Click **Add**, or select an existing entry and click **Edit** or **Delete**.
   b. (Add or Edit only), Specify the time interval for the schedule, as shown in Figure 10-18.

**Figure 10-19  Time Schedule Interval**

   c. Enter the **Start** and **End** time in hour and minute format (hh:mm)
   d. Select the **Days of Week** for the schedule.
   e. Select additional **Holidays** for the schedule.
   f. Click **Save and Close**.
   g. Repeat step a to step f Define additional time intervals, if necessary.

Step 6  Click **Save and Close** to save the changes in the detail window (Figure 10-18).
Configuring Alert Sounds

Alert sounds play when an alarm occurs (if the alarm is configured with one of the available sounds). This section includes instructions to add or modify the available sounds. For instructions to assign the sounds to an alarm type, see Modifying Default Event Policies, page 10-28.

To add or modify alert sounds, do the following:

Step 1  Select **Alert Sounds** module from the **Events & Alarms** menu, in the **Configuration** sub-menu.

Step 2  The main window (Figure 10-20) shows the currently defined alert sounds.

- To modify an existing alert sound, select the entry and choose **Edit**... to open the detail window. You can also double-click the entry.
- To add a new alert sound, click **Add**... to open the detail window.
- Click **Delete** to delete the selected entry.

![Figure 10-20 Alert Sound Module Main Window](image)

Step 3  Edit a new or existing alert sound using the detail window (Figure 10-21):

![Figure 10-21 Alert Sounds Module Detail Window](image)

a. Click **Import WAV File** and select a sound file from a local drive. Click **Play WAV File**... to preview the alert sound.

b. Enter a name for the alert sound.

c. Click **Save & Close**.
Setting Event and Alarm Priorities

Priorities are used to sort or filter events and alarms. To define the priorities for an event or alarm log code, edit the Priority setting for the Log Code using the Event Policy Manager:

**Step 1**
Open the Event Policy Manager module in the Events & Alarms: Configuration menu. Edit an event policy by selecting it and clicking the Edit... button in the tool bar. This opens the Event Policy window (Figure 10-22).

**Figure 10-22   Event Policy Window**

- **Log** code: CB.COP.REFRESH_CAMERAS.ERR
- **Log code description**: Cisco VSM Camera Driver command failed: Synchronize with Cisco VSM
- **Applies to**: Device Command Result
- **Log code category**: Any
- **Device**: Any
- **Partition**:
- **Classification**:
- **Anti-passback area**:
- **Anti-passback area (int)**:
- **Entrance**:
- **Zone**:
- **Hierarchical location**:
- **Device type**: Any
- **Priority**: 0
- **Alert sound**: Default
- **Recall alert sound**: Default
- **Background color**:
- **Foreground color**:

**Step 2**
Use the Priority drop-down arrow to change the priority of the event or alarm. Positive priorities are above normal priority, and negative priorities are below normal. Zero is normal.

**Step 3**
Click Save and Close to save your changes.
For more information, see Modifying Default Event Policies, page 10-28.
Defining User Privileges for Editing Events

To change the event fields to read-only, change the access privileges a the user profile:

**Step 1** Select **Profiles** in the **Users** menu.
**Step 2** Click **Add** or select an existing profile and click **Edit** (Figure 10-23).
**Step 3** Click the **Data Types** tab.
**Step 4** Click the Data Type that you want to edit. For example, **Badge**, **Personnel Record**, etc.
**Step 5** Select or deselect the options for **View**, **Create**, **Modify**, or **Delete**.
**Step 6** Click **OK** to save the changes.

*Figure 10-23   Selecting Editable Fields in the Profiles Module*
Using Graphic Maps

Graphic Maps provide a visual representation of the devices available in a location. Icons representing the devices provide real-time status and alarms information, and allow the user to trigger actions such as viewing live video or denying access to a door. Automated rules can also be invoked, and icons representing a location provide status and alarm summary for all the devices assigned to that location.

This section describes the map viewer, and the editor used to create the maps:

- Graphic Maps Viewer, page 10-39
- Graphic Map Editor, page 10-42

Graphic Maps Viewer

Select Graphic Maps Viewer in the Events & Alarms menu (in the Monitoring submenu).

Figure 10-24 shows a sample map. In the top left frame, click + and - to expand and collapse the map folders and view associated devices. Right-click a device to view the actions and commands available for that device.

Figure 10-24 Graphic Maps Viewer Main Window
Icon Colors and Status

On the map, icons representing devices, automated rules, and locations provide status information using two colors: the inside fill color and the outside ring color.

**Inside Fill Color**

The inside color represents the device state.

- **Light Green**: Represents armed, secure, online states.
- **Red**: Represents unknown, active, offline states.
- **Dark Blue**: Represents disarmed, inactive states.
- **Light Blue**: Represents disarmed, active.

**Outer Ring Color**

The outer ring color represents the alarm state.

- **Green**: Represents a normally operating device free of any alarms.
- **Orange**: Represents a device in an acknowledged alarm or alarms state.
- **Red**: Represents a device in an alarm state.

### Device Commands

Right-click an icon to view the available commands for that device. For example, you can view live video for a camera, or deny access for a door, depending on your access privileges.

**Tip** To trigger an automated rule, click the icon.

### Layers and Views

#### Layers

Layers allow you to hide or display categories of icons, depending on the map configuration.

Click the Layers tab in the bottom left of the window, then right click the layer title and select **Toggle Layer Visibility**.

For example, turn the Doors layer off to hide the door icons. Toggle the layer on to display the icons.
Layers that contain one or more devices have a + sign to the left of the layer icon, allowing it to be expanded to show the associated devices.

Views

Click the Views tab to select the available views. For example, one view may display an entire floor plan, while another view displays only the reception area.

**Toolbar and Navigation Controls**

Use the following menu controls to select maps and adjust the map display.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back Arrow</td>
<td>Navigates backwards in the viewed maps history.</td>
</tr>
<tr>
<td>Forward Arrow</td>
<td>Navigates forward in the viewed maps history.</td>
</tr>
<tr>
<td>Up Arrow</td>
<td>Navigates to maps linked to the displayed map.</td>
</tr>
<tr>
<td>All Maps</td>
<td>Opens a menu containing all maps for easy navigation regardless of whether the sidebar is shown.</td>
</tr>
<tr>
<td>Layers</td>
<td>Displays all layers in the open map, and allows you to show and hide layers, regardless of whether the sidebar is shown.</td>
</tr>
<tr>
<td>Views</td>
<td>Displays a selected map view, regardless of whether the sidebar is shown.</td>
</tr>
<tr>
<td>Hide/Show Sidebar</td>
<td>Hides/Shows the Maps, Layers, and Views tabs in the sidebar.</td>
</tr>
<tr>
<td>Print</td>
<td>Prints the currently displayed map.</td>
</tr>
<tr>
<td>Zoom</td>
<td>The zoom tool is located in the upper right of the <strong>Graphic Maps Viewer</strong>. Use the drop-down arrow to select a zoom percentage, or type in custom zoom percentage number and press Enter. To cancel the zoom and reset the view, use the zoom tool drop-down and select <strong>Reset</strong>, or right-click the map and click <strong>Reset View</strong>.</td>
</tr>
<tr>
<td>Zoom Marquee</td>
<td>To zoom a map to a specific rectangular area; hold down the Control button, click and drag a rectangle on the map. Release the mouse button and the map will zoom to fit the rectangle. To scroll the map hold down the Shift button, click the map and drag to a desired location.</td>
</tr>
</tbody>
</table>
Graphic Map Editor

Use the Graphic Map Editor to create facility maps and add icons that represent doors, cameras, locations and automated rules. Once configured, the maps are viewed using the Graphic Map Viewer.

**Caution**
Do not use the Graphic Maps Editor while other client workstations have the Graphic Maps Viewer or Graphic Maps Editor open. Use of the Graphic Maps Editor while any other client workstations have the Graphic Maps Viewer or Graphic Maps Editor opened may result in system errors.

To create or modify graphic maps, do the following:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select Graphic Map Editor from the Admin menu.</td>
<td>![Graphic Map Editor Menu]</td>
</tr>
</tbody>
</table>
| **Step 2** *(Optional)* Add a folder for map organization:  
  a. Click New Folder.  
  b. To rename the folder, right click the folder and select Folder Properties from the command menu. | ![New Folder] |
| **Step 3** Create a new map:  
  a. Click New Map.  
  b. Select a background image from a local drive. Background images are typically floor or building layouts.  
  **Tip** You can also select options to create folders and maps by right-clicking a map folder. | ![Create New Map] |
### Step 4
(Optional) Use the clip and zoom controls to adjust the image:

- **Clip**: use the Clip button to crop a map image. To clip a map, click the Clip button, click and drag a rectangle on the graphic map, and then click the Clip again to crop the map.

- **Zoom**: zoom in or out using the zoom tool in the upper right of the window. Click + or - to zoom in and out, select a zoom percentage, or enter the percentage in the box.

To cancel the zoom and reset the view, select [Reset](#) from the drop-down menu, or right-click the map and click [Reset View](#).

- **Zoom Marquee**: to zoom a map using the zoom marquee feature, hold down the Control button, click and drag a rectangle on the map. Release the mouse button and the map will zoom to fit the rectangle.

**Tip** To move a map hold down the Shift button, click the map and drag to a desired location. Navigate between modifications by using the [Undo](#) and [Redo](#) buttons.

### Step 5
(Optional) Right-click the map to access the following functions:

- **Reset View**: cancel a zoom view and return to 100%.

- **Change Background**: selects a new background image for the map.

- **Edit Map Properties**: defines the properties of the map, such as the icon scale.

- **Edit View Properties**: defines layout properties.

- **Toggle Layer Visibility**: turns layer visibility on or off.

- **Edit Layer Properties**: edits the layer name.
To do this | Use this display
--- | ---
**Step 6** Add a devices or doors to the appropriate location on the map.  
The the device will report real-time status in the Graphic Maps Viewer.  

- Click the **Devices** tab to view the Gateways, doors and drivers.
- Drag a device to an appropriate place on the map.

**Tip** To add Door Groups, click the **Device Groups** tab and drag the group to the map. See Configuring Device Groups, page 6-28 for more information.

**Step 7** Add locations to the map.  
The the device will report real-time status in the Graphic Maps Viewer.  

- Click the **Locations** tab.
- Drag a location to an appropriate place on the map.

**Tip** Click a Layer icon in the bottom left window to organize the map elements into different layers. For example, click a layer and add the devices, then click another layer and add locations or commands. You can turn layers on or off by right-clicking the layer and selecting **Toggle Layer Visibility**. Select Edit Layer Properties to rename the layer. A green check indicates the active layer (the layer that new icons will be added to).
Chapter 10  Events & Alarms

Using Graphic Maps

<table>
<thead>
<tr>
<th>Step 8</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add commands to the map. Users can click on command icons in Graphic Maps Viewer to invoke the command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Click the Commands tab to view the commands available for the selected device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Drag a command to the map. The Device Command window opens.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Click OK to accept the selected command and add it to the map.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>(Optional) To select a different device and command combination using the Device Command window, do the following:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Select the device(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Single: click Choose and select a single device or door from the Hardware view, as shown in the example to the right.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Multiple (by filter) of type: select a device type from the drop-down menu. To refine the selection, click Filter and select the filter options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Multiple (by group) of type: select a device group from the drop-down menu.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Select a command for the device(s): click Choose and select a command from the list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. (Optional) Click Choose to select the Parameters for the command, if required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If Choose is shown in black, you must click the button to continue. Select a parameter from the list. If the message “Are you sure you want to continue?” appears, click OK. This message indicates that a parameter is not required.</td>
<td></td>
</tr>
<tr>
<td>d. Click OK.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 10      Events & Alarms

**Using Graphic Maps**

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong> (Optional) Add automated rules to the map.</td>
<td>![Image of a map with a Device Command window and a note about selecting the Automation Driver and Invoke Automation Rule.]</td>
</tr>
<tr>
<td>a. Click the <strong>Devices</strong> tab and select the <strong>Automation Driver</strong>.</td>
<td></td>
</tr>
<tr>
<td>b. Click the <strong>Command</strong> tab and drag the icon for <strong>Invoke Automation Rule</strong> to the map. The Device Command window appears.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> In the Device Command window, the selected device is <strong>Automation Driver</strong>, and the selected command is <strong>Invoke Automation Rule</strong>.</td>
<td></td>
</tr>
<tr>
<td>c. To select the rule, click <strong>Choose</strong> in the Parameters field and select the rule. To define rules, see Configuring Automated Tasks Using Global I/O, page 11-14.</td>
<td>![Image of a Device Command window with a selected rule.]</td>
</tr>
</tbody>
</table>

| **Step 11** (Optional) Create multiple views of the map. | ![Image of a map with a Map View window and instructions for adjusting view properties.] |
| a. Zoom and position the map to focus on a specific area or set of devices. | |
| b. Click **View** in the top menu bar. | |
| c. Use your mouse to click and drag a border within the map. | |
| d. Release the mouse button to select the area. The Map View window appears. | |
| e. Adjust the View properties, if necessary. Click **Make default view** to make the view the default when the map is opened in the Graphic Map Viewer. | |
| f. Click **OK** to save the changes and create the new view. | |
| g. To change the name and other settings, right-click the view name and select **Edit View Properties**. | |

| **Step 12** (Optional) Edit the icon properties. | ![Image of a map icon with Edit Icon Properties window.] |
| Right-click a map icon and select **Edit Icon Properties**. | |
| To change the icon image, click **Choose** in the Image section of the Properties window. | |

| **Step 13** Click **Save**. Changes are visible in the Graphic Maps Viewer only after they are saved. | ![Image of a Save button clicked on a map.] |
Archiving Historical Events

Historical events are old events or alarms that you wish to remove from the main database. Archiving historical events are removed from the live Events & Alarms listings. This can improve system performance and simplify system monitoring since only the latest, most relevant, events and alarms are displayed.

There are three steps to archiving historical events:

1. **Copy historical events**: copies old events to a separate Cisco PAM database table. The events are still visible in Cisco PAM Events & Alarms. They are also included in system backups, and you can run reports on the events.

2. **Prune historical events**: deletes copied events from the main database table. The historical events are still in the Cisco PAM database, but are not visible in Events & Alarms. The historical events are still included in system backups, and you can run reports on the events.

3. **Archive historical events**: creates a compressed, password-protected file of the historical events, and deletes the events from the Cisco PAM database. This can significantly reduce the size of the Cisco PAM database and backup file.

   The archive file can be copied to another location, and restored to the Cisco PAM database if necessary. The file can also be used by other applications to view old events or run reports. In addition, the historical event records are self-contained: referenced objects, such as a person’s name and card number, are retained even if the original record is deleted. Reports on historical events can also span a much longer time range than is normally possible for live events.

To copy, prune, and archive historical events, enable the Historical Events driver. You can use the driver commands to copy and prune old events, or create an automated task to perform these actions on a regular schedule.

This section includes the following instructions:
- Using Driver Commands to Copy and Prune Historical Events, page 10-48
- Creating an Automated Rule to Archive Historical Events, page 10-51
- Creating Reports from the Historical Events Archive, page 10-55

**Tip**

For instructions to backup Cisco PAM data and configurations, or create a .zip archive of historical events, see Appendix A, “Backing Up and Restoring Data.”
# Using Driver Commands to Copy and Prune Historical Events

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
</table>
| **Step 1** | ![Driver Manager](image1)  
Enable the Historical Events driver.  
- Select **Hardware** from the Doors menu.  
- Right-click the Driver Manager, and select **New Historical Events Driver**...  

| **Step 2** | ![Live events window](image2)  
Enter the number of days that events remain in the live events database before they are moved to the historical events database.  
  
a. Click the **Driver** tab.  
b. In **Live events window (days)**, enter the number of days. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are moved to the historical events.  
  
**Note**  
The number is rounded to midnight of the last day.  
c. Click **Save and Close**.  

| **Step 3** | ![Driver Manager](image3)  
Right-click the driver and select **Start**.  

| **Step 4** | ![Driver Manager](image4)  
Right click the driver and select **Start Copying Live Events**.  
This process copies old events to the historical events database. The events are still in the main database.  
**Tip**  
Perform these commands during off-peak hours to avoid impact to system performance. |
### Archiving Historical Events

**Step 5** Right click the driver and select **Stop Copying Live Events**.

This stops the process. If you do not stop the process, copying continues indefinitely and impacts system performance. Allow a sufficient amount of time for the copy process to complete.

See [Creating an Automated Rule to Archive Historical Events, page 10-51](#) to create an automated process that invokes these commands on a set schedule.

**Step 6** Right click the driver and select **Start Pruning Live Events**. The following conditions apply:

- Pruning will fail if any events or alarms have pending actions (such as an automated rule). Select the **Clean up queues** command to clear actions for old events or alarms.
- Pruning deletes events from the live events database only if they were copied to the historical events database.
- Alarms are deleted only if all alarm duplicates and annotations are past the live events time.

**Tip** Perform these commands during off-peak hours to avoid impact to system performance.

**Step 7** Right click the driver and select **Stop Pruning Live Events**.

This stops the pruning process. If you do not stop the process, pruning continues indefinitely and impacts system performance. Allow a sufficient amount of time for the pruning process to complete.

See [Creating an Automated Rule to Archive Historical Events, page 10-51](#) to create an automated process that invokes these commands on a set schedule.
<table>
<thead>
<tr>
<th><strong>To do this</strong></th>
<th><strong>Use this display</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td>Verify that event pruning was successful, and clear the event queue, if necessary.</td>
</tr>
</tbody>
</table>
| **Events** or alarms that have a dependant action (such as an automated rule), cannot be pruned. For example, if the related device (such as a Gateway) is disabled or deleted, then the event will not clear and pruning will fail. To clear these events and allow pruning to continue, invoke the **Clean up queues** command, as described in the following example: | ![Events - Cisco Physical Access Manager](image1)
| a. Select **Events** from the **Events & Alarms** menu, under the **Monitoring** sub-menu. | ![Events - Cisco Physical Access Manager](image2)
| • In the example to the right, the second event from the bottom reads “Successfully pruned 0 events”. This means that the events could not be pruned since one or more events have a dependant action (such as an automated rule). | ![Events - Cisco Physical Access Manager](image3)
| b. To clear any dependencies for the events, right-click the Historical Events Driver and select the **Clean up queues** command. | ![Events - Cisco Physical Access Manager](image4)
| c. Verify that the events were pruned. In the example to the right, the event outlined in green reads “Successfully pruned 2554 events”. This indicates that the historical events were successfully pruned. | ![Events - Cisco Physical Access Manager](image5)
| **Step 9** | (Optional) Archive the historical events database to remove old events from the main database. |
| **Archive the historical events database to remove old events from the main database.** See **Appendix A, “Backing Up and Restoring Data”** for more information. | ![Events - Cisco Physical Access Manager](image6)
Creating an Automated Rule to Archive Historical Events

To automatically move old events from the live events database to the historical events database, create automated rules to copy and prune old events. Create automated rules to clean up the event queues, start and stop copying, and then start and stop pruning, in that order.

Choose task times that minimize system impact but considers the latency between when an event occurs and when it is available in the historical events table.

- If performance is critical and latency is not, configure copying and pruning during off-peak hours.
- If low latency is important, and the copying and pruning does not impact system performance, configure the actions to occur around the clock.

Tip
Schedule data backups to occur after event pruning is complete to reduce the amount of data to be backed up. See Appendix A, “Backing Up and Restoring Data” for instructions.

The following instructions describe how to create the automated tasks to copy and prune historical events. For example, create a rule for each of the following tasks:

- Rule 1: 6:30 PM Clean Up Queues
- Rule 2: 7:00 PM Start Copying Live Events
- Rule 3: 12:30 AM Stop Copying Live Events
- Rule 4: 1:00 AM Start Pruning Live Events
- Rule 5: 6:00 AM Stop Pruning Live Events

Step 1
Enable the Historical Events Driver, if necessary.

a. Select Hardware from the Doors menu.
b. Right-click the Driver Manager, and select New Historical Events Driver....
c. Enter the number of days that events remain in the live events database before they are moved to the historical events database.
   - Click the Driver tab.
   - In Live events window (days), enter the number of days. For example, enter 30 to keep events in the live view for 30 days. After midnight on day 30, the events are moved to the historical events. The number is rounded to midnight of the last day.
   - Click Save and Close.
d. Right-click the driver and select Start.
See Using Driver Commands to Copy and Prune Historical Events, page 10-48 for more information.
To do this | Use this display
--- | ---
**Step 2** | Enable the Automation Driver, if necessary.
See [Enabling the Automation Driver, page 11-12](#) for more information.

**Step 3** | Select **Global I/O** from the **Events & Alarms** menu. The Automates Rules window opens and lists the currently defined rules.

**Step 4** | Click **Add** to create a new automated rule.

**Step 5** | Enter a name and schedule for the rule.

   a. **Name**: enter a descriptive name for the rule. For example, *Clean up event queues*.
   b. Click **New** to create a new Trigger.
   c. In the Trigger Type window, select **Periodic** and then click **OK**.
   d. In the Periodic window, select the Interval: **Monthly**, **Weekly**, or **Daily**.
   e. Select the day of week or day of month, if necessary, and the **Time of day** (in a 24-hour format).
   f. Click **OK**.

**Step 6** | Create an action to execute a command:

   a. In the Actions section, click **Add**.
   b. Select **Device Command** and click **OK**.
### Step 7
Select the device driver and associated command:

- **a.** Select **Single** in the Device(s) section.
- **b.** Click **Choose** and then select the **Historical Events Driver**. Click **OK**.
- **c.** Select a command. Click **Choose** and then select the command. For example, select **Start Copying Live Events**. Click **OK**.
- **d.** Click **Save and Close** to close the Device Command window. The action is added to the Actions list.

### Step 8
(Optional) Specify the notification and event options, if necessary.

See **Configuring Global I/O Automated Rules**, page 11-12 for more information.

### Step 9
Click **Save and Close** to create the rule and add it to the rules list.
### Archiving Historical Events

**Step 10**

Repeat these steps for each command. Create separate commands to stop and start copying and stop and start pruning. For example:

- Rule 1: 6:30 PM Clean Up Queues
- Rule 2: 7:00 PM Start Copying Live Events
- Rule 3: 12:30 AM Stop Copying Live Events
- Rule 4: 1:00 AM Start Pruning Live Events
- Rule 5: 6:00 AM Stop Pruning Live Events

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Display of Management Console" /></td>
</tr>
</tbody>
</table>

*To do this:* Use this display
Creating Reports from the Historical Events Archive

To run reports on historical events that were copied to the historical events database, create a filter-based report in the Report Manager.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Select Report Manager from the Reports menu.</td>
<td><img src="Image" alt="Report Manager" /></td>
</tr>
<tr>
<td>Step 2: Click Add and select Add Filter-based Report Template.</td>
<td><img src="Image" alt="Add Filter-based Report Template" /></td>
</tr>
<tr>
<td>Step 3: Select the template settings:</td>
<td><img src="Image" alt="Add Filter-based Report Template Settings" /></td>
</tr>
<tr>
<td>• Name: the name of the report.</td>
<td></td>
</tr>
<tr>
<td>• Max results: the number of results displayed in the report. -1 is unlimited results.</td>
<td></td>
</tr>
<tr>
<td>• Item type: select Events (Historical).</td>
<td></td>
</tr>
<tr>
<td>• Edit Filter: the filter setting, similar to filters available in the toolbar. See Using Filters, page 3-12.</td>
<td></td>
</tr>
<tr>
<td>• Report Settings: Report generation options, which are the same as when generating a report from one of the other modules. For more information see Creating Reports, page 3-10.</td>
<td></td>
</tr>
<tr>
<td>• Variable Parameters: information the user is be prompted to provide when the report is run.</td>
<td></td>
</tr>
<tr>
<td>• Edit Columns: the columns used in the report. Use the Up and Down buttons to reorder the columns for the report.</td>
<td></td>
</tr>
<tr>
<td>Step 4: Click Save and Close.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 11

Configuring Automated Tasks

This chapter describes how to create and manage automated tasks such as triggering a relay when an alarm is generated, playing an alarm video, or sending an event e-mail. In addition, you can create Quick Launch buttons for commonly used actions, and organize the buttons into different panels.

Contents

- Creating Quick Launch Buttons, page 11-2
  - Creating a Button, page 11-2
  - Creating a Button That Runs An Automated Rule, page 11-7
  - Creating Panels (Windows) of Related Buttons, page 11-7
  - Restricting User Access to Button Panels, page 11-8
- Configuring Device Automated Rules, page 11-9
- Configuring Global I/O Automated Rules, page 11-12
  - Enabling the Automation Driver, page 11-12
  - Configuring Automated Tasks Using Global I/O, page 11-14
  - Example: Automated Weekly Report, page 11-21
- Defining Reports (Report Manager), page 11-25
  - Using the Report Manager, page 11-26
  - Filter-based Report Template, page 11-27
  - Object SQL-based Report Template, page 11-28
  - SQL-Based Report Template, page 11-29
Creating Quick Launch Buttons

Quick Launch buttons provide one-click access to commonly used actions. For example, you can create buttons to unlock a door or open a Cisco PAM module. Complete the following instructions to create or modify buttons, and organize them into different panels (windows).

- Creating a Button, page 11-2
- Creating a Button That Runs An Automated Rule, page 11-7
- Creating Panels (Windows) of Related Buttons, page 11-7
- Restricting User Access to Button Panels, page 11-8

Creating a Button

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>Quick Launch</strong> from the Events &amp; Alarms menu, in the Monitoring sub-menu. The Quick Launch window opens.</td>
</tr>
<tr>
<td>Note</td>
<td>The Quick Launch window appears blank on first use since no Quick Launch icons have been created.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select <strong>Add Widget</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select a widget type to create a Quick Launch button. The widget types include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open Module</strong>: creates a button that opens a Cisco PAM module window.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Device Command</strong>: creates a button that executes a command for a door or device. For example, grant access to a door.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Label</strong>: Creates a text label used to organize Quick Launch buttons into rows and columns.</td>
</tr>
</tbody>
</table>
**To do this** | **Use this display**
---|---
**Step 4** | ![Add - Device Command Widget](image)
Select the row and column where the button will appear in the Quick Launch window. Select the **Locations** tab and enter the row and column number.

**Note** If another button already exists in that location, the existing button location automatically shifts to the right.

**Step 5** | ![Add - Device Command Widget](image)
Enter the text label for the button. You can also optionally select a custom icon image.

**Note** If the widget type is **Label**, enter only the label text, then skip to **Step 10**.

a. Click the **Appearance** tab.
b. **Label**: select the text label for the button.
   - **Default**: the default text. For example, the name of the device and command.
   - **None**: no text label. Only the icon image appears. If no icon image is selected, a blank button is displayed.
   - **Custom**: enter a custom name for the button.
c. **Image**: (Optional) Select a button icon image.
   - **Default**: the default icon image.
   - **None**: no button image. Only the text label appears. If no label is selected, a blank button is displayed.
   - **Custom**: click choose to select a custom image file.
Creating Quick Launch Buttons

<table>
<thead>
<tr>
<th>Step</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
</table>
| **Step 6** | If the widget type is **Open Module**, select a module:  
  a. Click the **Open Module** tab.  
  b. Select the Cisco PAM module that will open when the Quick Button is clicked.  
  c. Click **OK**.  
  d. Skip to **Step 10**. | ![Add Open Module Widget](image1) |
| **Step 7** | If the widget type is **Device Command**, select the door or device for the command:  
  a. Click the **Device Command** tab.  
  b. Select the device(s):  
    - **Single**: click **Choose** and select a single device or door from the Hardware view, as shown in the example to the right.  
    - **Multiple (by filter) of type**: select a device type from the drop-down menu. For example, select **deadbolt** to select all deadbolt devices in all doors. To refine the selection, click **Filter** and select the filter options.  
    - **Multiple (by group) of type**: select a device group from the drop-down menu. Groups include:  
      - **Access Point**  
      - **Door**: select a Door Group. See  
      - **Monitor Point**  
      - **Monitor Point Group** | ![Add Device Command Widget](image2) |
### Chapter 11      Configuring Automated Tasks

#### Creating Quick Launch Buttons

<table>
<thead>
<tr>
<th>Step 8</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select a command for the door or device(s):</td>
<td><img src="image1.png" alt="Image of Quick Launch setup" /></td>
</tr>
<tr>
<td></td>
<td>a. Select <strong>Choose</strong>.</td>
<td><strong>Tip</strong> See Device and Driver Commands in the Hardware Device View, page 6-34 and Door Modes and Commands, page 6-39 for command descriptions.</td>
</tr>
<tr>
<td></td>
<td>b. Select a command from the list. For example, <strong>Deactivate Access Levels</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**Tip**

<table>
<thead>
<tr>
<th>Step 9</th>
<th>a. Click <strong>Choose</strong> to select the Parameters for the command, if required.</th>
<th><img src="image2.png" alt="Image of parameter selection" /></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If <strong>Choose</strong> is shown in black, you must click the button to continue. Select a parameter from the list. If the message “Are you sure you want to continue?” appears, click <strong>OK</strong>. This message indicates that a parameter is not required.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>OK</strong>. The new button appears on the main Quick Launch page.</td>
<td></td>
</tr>
</tbody>
</table>
Step 10 (Optional) Repeat these steps to create additional quick launch buttons, or organize the buttons in the current panel (window).

- To edit an existing button (widget), right-click the button, select **Edit**, and edit the properties as necessary.
- To move the buttons on the page, do one of the following:
  - Right-click the button and select **Move Left**, **Move Right**, **Move Up**, or **Move Down**.
  - Right-click the button, select **Edit** and then **Location** to select the row and column.

Step 11 (Optional) Create panels (windows) of related buttons.
Creating a Button That Runs An Automated Rule

Create a button that runs an automated rule.

**Step 1** Select *Add Widget* and then *Device Command*.

**Step 2** Click *Choose* to select a single device.

**Step 3** In the Hardware view, select the *Automation Driver*, and then click *OK*.

**Step 4** Click *Choose* next to the Command field, click *Choose*.

**Step 5** Select *Invoke Automation Rule* and click *OK*.

**Step 6** Click *Choose* next to the Parameters field, select a Rule, and then click *OK*.

**Step 7** Click *OK* to save the changes and close the window.

See *Configuring Global I/O Automated Rules*, page 11-12 for more information.

Creating Panels (Windows) of Related Buttons

**Step 1** Create one or more Quick Launch buttons.

**Step 2** Select *Save* or *Save As* to save the current Quick Launch window as a panel.

**Step 3** Enter the panel name.

**Step 4** Click *OK*.

**Tip** To toggle between the panels, select *Panels* from the menu bar and select a panel.
Restricting User Access to Button Panels

Restrict user access to the button panels using the Profiles and Login modules, as described in the following instructions.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create or modify profiles to include the required Quick Launch access privileges. Profiles are sets of access privileges that are assigned to individual user logins.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Open the Profiles module.</td>
</tr>
<tr>
<td>b.</td>
<td>Click Add or Edit to create or modify a profile.</td>
</tr>
<tr>
<td>c.</td>
<td>Click the Module tab.</td>
</tr>
<tr>
<td>d.</td>
<td>Click Quick Launch.</td>
</tr>
</tbody>
</table>
| e.     | Select the options to the right:  
  - Allow access to module: allow profile users to access the Quick Launch module.  
  - Allow edit: allow users to create and edit buttons.  
  - Allow all panels: allow access to all panels. Uncheck this option to enable the following button.  
  - Choose allowed panels: select the panels that can be accessed by this profile. |
| f.     | Click Save and Close. |

Tip: For more information, see Chapter 4, “Configuring User Access for the Cisco PAM Desktop Client”.

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Assign the profile to the user login.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Open the Login module.</td>
</tr>
<tr>
<td>b.</td>
<td>Click Add or Edit to create or modify a user login.</td>
</tr>
<tr>
<td>c.</td>
<td>Select Profiles.</td>
</tr>
<tr>
<td>d.</td>
<td>Select the profile that includes the required access privileges.</td>
</tr>
<tr>
<td>e.</td>
<td>Click Save and Close.</td>
</tr>
</tbody>
</table>
Configuring Device Automated Rules

Use the **Device I/O Rules** module to create event based rules for a specific Gateway and the doors and devices configured on the Gateway. For example, when a door is forced open, a rule can activate a generic output device to sound an alarm. Since device rules are implemented for a single Gateway, the action is triggered immediately.

Device automation rules differ from global automation rules (Global IO) in the following ways:

- Device rules affect a single Gateway. Global IO rules can affect multiple Gateways.
- Device rules trigger actions immediately since they are executed on the Gateway and not subject to system or network delays. Global IO rules may not execute immediately due to network delays, rules processing, communication between Cisco PAM and the Gateways, or other factors. See **Configuring Global I/O Automated Rules**, page 11-12 instructions to create global rules.

Complete the following instructions to create or modify Device IO Rules:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><img src="image1" alt="Device I/O Rules" /></td>
</tr>
<tr>
<td>Select <strong>Device IO Rules</strong> from the Doors menu.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

Click **Add**, or select an existing rule and click **Edit**.

To duplicate an existing rule:

- Select the entry and click the **Duplicate** button in the upper right of the main window.
- Enter a **New Name** for the rule and click **OK**.
- In the main window, select the duplicate rule name and click **Edit**.
- Revise the rule settings as described in the following steps.
### Configuring Device Automated Rules

**Step 3**

Enter the rule settings:

- **Name**: enter the name of the rule.
- **Description**: enter a short description of the rule.
- **Gateway**: select the Gateway where the device is installed.

**Trigger**

- **Device Type**: select the device type:
  Door, Generic Input device, Glass Break Sensor, Motion Sensor, Duress Sensor, Fire Sensor, Tamper device or Power Fail device.
- **Device**: select the device name.
- **Event**: select the event type. When this event occurs on the selected device, the following action is performed.

**Action**

- **Device**: select the device for the action.
- **Command**: Select the device command. For more information, see Device and Driver Commands in the Hardware Device View, page 6-34.

**Step 4**

Click **Save and Close** to save the changes. The new or revised rule is displayed in the main window.
Step 5

Select **Apply Configuration Changes** on the affected Gateway to activate the rule.

**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.

You can apply changes using either the Hardware or Locations & Doors module:

**Hardware module**

- Right-click the *Access GW Driver* and select **Apply Configuration Changes** to download configuration changes for all Gateways.

  or

- Right-click on a *Gateway Controller* and select **Apply Configuration Changes** to download configuration changes for a single Gateway.

**Locations & Doors module**

a. Select *Gateway Controllers* from the *View* menu to display the Gateways.

b. To download the configuration for a multiple devices, right-click a location and select **Apply Configuration Changes**.

  or

c. Right-click a Gateway icon and select **Apply Configuration Changes** to download the configuration for a single device.

See **Applying Configuration Changes**, page 6-17 for more information.
Configuring Global I/O Automated Rules

Automated rules can execute commands, generate event reports, edit multiple records, or perform URL actions. Once created, you can invoke the automated rules from other modules, such as Quick Launch buttons and Graphic Maps. Create automated tasks using the Global I/O module, as described in the following sections.

- Enabling the Automation Driver, page 11-12
- Configuring Automated Tasks Using Global I/O, page 11-14
- Example: Automated Weekly Report, page 11-21

Enabling the Automation Driver

To enable automated tasks, the Automation Driver must be created and configured in the Hardware window. The driver is only created once and remains active unless deactivated.

Tip

The Automation Driver is a system component that executes automation policy actions. See Viewing Doors and Devices in the Hardware View, page 5-3 for a description of the various system drivers.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Select <strong>Hardware</strong></td>
<td><img src="image1" alt="Hardware Menu" /></td>
</tr>
<tr>
<td>from the <strong>Doors</strong></td>
<td></td>
</tr>
<tr>
<td>menu.</td>
<td></td>
</tr>
</tbody>
</table>

| Step 1              |                  |
| Right-click the **Driver Manager** and select **New Automation Driver**... | ![Driver Manager](image2) |
Step 2
Enter the driver settings:

a. Click the General tab and enter a Name for the Automation Driver.

b. If e-mail notification is needed, click the SMTP Server Settings tab and enter the SMTP server settings.

c. Click Save and Close to close the configuration window and create the Automation Driver.

Step 3
Right-click the Automation Driver and select Start.
This enables the driver and activates any automated rules.
Configuring Automated Tasks Using Global I/O

Create automated rules to automatically execute commands, generate event reports. The automated rules can also be configured for manual use, useful when placing a task icon in a graphic map.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>Global I/O</strong> from the <strong>Events &amp; Alarms</strong> menu. The Automates Rules window lists the currently defined rules. The main window includes the following columns.</td>
</tr>
<tr>
<td><strong>Name</strong>: The name of the automated task.</td>
<td><img src="image1.png" alt="Global I/O" /></td>
</tr>
<tr>
<td><strong>Enabled</strong>: Yes if the task is enabled. No if the task is disabled.</td>
<td><img src="image2.png" alt="Global I/O" /></td>
</tr>
<tr>
<td><strong>Trigger</strong>: Operator-defined events, and or time schedules that execute an action or notification.</td>
<td><img src="image3.png" alt="Global I/O" /></td>
</tr>
<tr>
<td><strong>Action</strong>: Reporting or device commands executed on devices.</td>
<td><img src="image4.png" alt="Global I/O" /></td>
</tr>
<tr>
<td><strong>Notification</strong>: The notification type. For example: E-mail, FTP, or Syslog notification.</td>
<td><img src="image5.png" alt="Global I/O" /></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Add</strong>, or select an existing rule and click <strong>Edit</strong>. <strong>Tip</strong> You can also right click to select an option.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter a Name for the rule and select or deselect the Enabled checkbox.</td>
</tr>
</tbody>
</table>
## Chapter 11      Configuring Automated Tasks

### Configuring Global I/O Automated Rules

#### Step 4
Enter a **Trigger** type for the rule.

Click **New** or **Edit** to define the Trigger Type. The choices are:

- **Event**: The rule is invoked when an event matching the defined filter occurs.
  - Select Event.
  - Click **Edit Filter** to define the filter.
  - Select a **Time Schedule** for the rule. If the event occurs within the specified schedule, the rule will be invoked. See **Configuring Time Schedules**, page 10-34 to define the schedules.

- **Periodic** (time schedule): The rule is invoked according to a **Monthly**, **Weekly**, or **Daily** schedule. Select the day of week or day of month, if necessary, and the **Time of day** (in a 24-hour format).

- **Manual Only**: The rule is invoked manually. You can create a Quick Launch button or add the rule to a graphic map.

#### Step 5
Define one or more **Actions** that occur when the rule is triggered. The options are:

- **Report**: Generates a report that can be saved or sent to a user.

- **Device Command**: Executes a command on a specified device.

- **CSV Import**: Imports a *comma separated value* file containing personnel, organization, or access level data. The file must be located on an FTP server.

- **Group Edit**: Edits multiple personnel or badge records.

- **Sanity Report Action**: Provides a snapshot of the system status.

- **URL Action**: performs a pre-defined URL action.

**Tip**  See **Understanding Automated Rule Actions**, page 11-17 for descriptions of the fields and settings for each option.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> Enter a <strong>Trigger</strong> type for the rule. Click <strong>New</strong> or <strong>Edit</strong> to define the Trigger Type.</td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Step 5</strong> Define one or more <strong>Actions</strong> that occur when the rule is triggered.</td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
</tbody>
</table>
Step 6 Specify a **Notification** option to define where the notification or report file is sent. The options are:

- **E-mail**: Sends the notification or report file to one or more e-mail addresses. To enable e-mail notifications, you must enter the SMTP server settings in the Automation driver. For instructions, see *Enabling the Automation Driver*, page 11-12.

- **FTP**: Sends the file to the specified FTP server.
  - **Host**: The FTP server IP address or name.
  - **Username**: Log in username required by the FTP server.
  - **Password**: Password to log in to the FTP server.
  - **Path**: Path on the FTP server where files should be uploaded.

- **Syslog**: Sends the notification or report to a Syslog.
  - **Host**: The Syslog server IP address or name. You must verify that the server is accessible and allows remote hosts to log messages. Cisco PAM does not verify the Host server availability.
  - **Facility**: The log facility to use when recording the information to the Syslog.

Step 7 Select the event options. These events occur when the rule is successfully invoked, or when rule options fail.

Click the check boxes to activate or deactivate the options:

- **Record event when rule invoked**: Each time the rule is invoked, record an event.

- **Record event when trigger fails**: Each time the trigger fails, record an event.

- **Record event when action fails**: Each time the action fails, record an event.

- **Record event when notification fails**: Each time the notification fails, record an event.

Step 8 Click **Save and Close**.
Understanding Automated Rule Actions

Automated rule actions define what occurs when the rule is triggered. Actions are defined when creating or editing a rule, as described in Step 5 of Configuring Automated Tasks Using Global I/O.

Each automated rule option is described in the following table:

- **Report**: Generates a report that can be saved or sent to a user.
- **Device Command**: Executes a command on a specified device.
- **CSV Import**: Imports a comma separated value file located on an FTP server. The file can contain personnel, organization, or access level data.
- **Group Edit**: Edits multiple personnel or badge records.
- **Sanity Report Action**: Provides a snapshot of the specified system status.
- **URL Action**: Performed a pre-defined URL action.

Create or edit an automated rule as described in Configuring Automated Tasks Using Global I/O, page 11-14. In the Actions section, click Add to create a new action, or select an existing action and click Edit.

---

**Report**

Generates a report that can be saved or sent to a user. Complete the following settings:

a. Select the Action type Report.

b. Click Choose to select a predefined report template. To create or modify reports, see Defining Reports (Report Manager), page 11-25.

c. Click Settings to define the report:

   - Title: edit the name of the report, if necessary.
   - Group by: select the group, if available.
   - Format: select Record-style or Table-style.
   - Output type: select an output type from the drop-down menu. For example: PDF document.
Configuring Global I/O Automated Rules

Device Command
Executes a command on one or more devices:

a. Select the Action type **Device Command**.

b. Device(s): Select the Device(s):
   - **Single**: click **Choose** and select a single device or door from the Hardware view.
   - **Multiple (by filter) of type**: select a device type from the drop-down menu. For example, select **deadbolt** to select all deadbolt devices in all doors. To refine the selection, click **Filter** and select the filter options.
   - **Multiple (by group) of type**: select a device group from the drop-down menu. To create door groups, see Configuring Device Groups, page 6-28.
   - **Variable (of type)**: select a device type from the drop-down menu and then click **Variable** to select a variable.

   For example, select the variable type **Door**, and then click the **Variable** button. Select **Triggering Event: Device** from the drop-down menu and click **OK**. If a the event Trigger configured in Step 4, page 11-15 is caused by a door, then the action is initiated.

c. **Command**: Click **Choose** to select the Command for the device(s). See Device and Driver Commands in the Hardware Device View, page 6-34 and Door Modes and Commands, page 6-39 for command descriptions.

d. **Parameters**: (Optional) Click **Choose** to select the Parameters for the command, if required.

   **Note** If **Choose** is shown in black, you must click the button to continue. Select a parameter from the list. If the message **“Are you sure you want to continue?”** appears, click **OK**. This message indicates that a parameter is not required.

e. **Click OK**

f. **Click Save and Close**.
CSV Import

Imports a comma separated value file from a file located on an FTP server.

**Note** The properties import file must be named csv.import.properties.

**Note** Do not include the header row in CSV import files. Otherwise, the header row is imported as data and results in one record more than the correct count.

**Note** To import pictures, the path name in the CSV file should be relative to the Directory path for the CSV properties file. If only the image name is specified in the CSV file, then the images must be located in the same directory as the CSV properties file.

- Select the Action type **CSV Import**.
- Select the data Type: Personnel, Organizations or Access Levels.
- Enter the server and file settings:
  - **Host**: the IP address of the FTP server.
  - **Username**: the username required for access to the FTP server.
  - **Password**: the FTP server password.
  - **Directory path**: the directory path for the file location.
  - **Configuration file**: (read-only). the import file must be named csv.import.properties.
- Click **Save and Close**.

Group Edit

Edits multiple personnel or badge records.

- Select the Action type **Group Edit**.
- Select the Item Type: for example, Badges.
- (Optional) Click **Edit Filter** to apply the changes to a subset of badges or records. Use the filter window to define the filter settings.
- Click **Group Edit** to enter the changes that will apply to all specified personnel or badge records.
- Click **Save and Close**.
Sanity Report Action

System sanity reports provide information about potential system inconsistencies or issues in the access control system. See Generating a System Sanity Report, page 5-16 for more information.

a. Select the Action type **Sanity Report Action**.
b. Select the Report type: for example, **Devices/Doors - Disabled**.
c. Click **Save and Close**.

URL Action

Performs a pre-defined URL action.

a. Select the Action type **URL Action**.
b. Select a pre-defined URL Action from the drop-down menu.
c. (Optional) Click **New** or **Edit** to create or modify a URL action. See Configuring URL Actions, page 12-2 for more information.
d. Click **Save and Close**.

Tip

Static URL actions can be invoked by creating a manual automated rule. Set the Trigger Type to **Manual** and Action Type as **URL Action**. Then select a static URL from the list. This rule can be invoked by right clicking on the Automation Driver in the Hardware module and selecting **Invoke Automation Rule**. You can also create a Quick Launch button to invoke the rule (see Creating Quick Launch Buttons, page 11-2).
## Example: Automated Weekly Report

The following sample shows how to configure an automated rule that runs a report on a weekly basis.

<table>
<thead>
<tr>
<th>Step</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>Global I/O</strong> in the Events &amp; Alarms menu.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a new rule and enter the General settings:</td>
<td><img src="image" alt="Automation Rule window" /></td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Add...</strong> to open the <strong>Automation Rule</strong> window.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. <strong>Name</strong>: Enter a descriptive name for the rule. For example: <strong>Daily Gateway Report</strong> (output).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. <strong>Enabled</strong>: Verify that the <strong>Enabled</strong> checkbox is selected.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the periodic Trigger to have the report sent at a regular scheduled time:</td>
<td><img src="image" alt="Select Trigger Type" /></td>
</tr>
<tr>
<td></td>
<td>a. From the Trigger row, click the <strong>New...</strong> button.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Periodic</strong> from the drop-down menu.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Select <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select the days and times for the periodic Trigger:</td>
<td><img src="image" alt="Periodic" /></td>
</tr>
<tr>
<td></td>
<td>a. <strong>Interval</strong>: Options include: <strong>Monthly</strong>, <strong>Weekly</strong> and <strong>Daily</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. <strong>Day of Week/Month</strong>: If you select <strong>Monthly</strong> or <strong>Weekly</strong>, select the day of the month or week.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. <strong>Time of day</strong>: Enter a time using a 24-hour notation. For example, 1:00 p.m. in a 12-hour clock is expressed as 13:00 in a 24-hour clock.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Select <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Select the action to generate a report file:</td>
<td><img src="image" alt="Select Action Type" /></td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Action</strong> section, click the <strong>Add...</strong> button.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Report</strong> from the drop-down menu.</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 11  Configuring Automated Tasks

#### Configuring Global I/O Automated Rules

**Step 6**  Define the type of report and the format of the output:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. From the Report window, click <strong>Choose...</strong>. The <strong>Choose Report</strong> window displays all reports defined in the system.</td>
<td><img src="image1.png" alt="Choose Report" /></td>
</tr>
<tr>
<td>- Select a report from the list.</td>
<td><img src="image2.png" alt="Choose Report" /></td>
</tr>
<tr>
<td>- Click <strong>OK</strong> to close the <strong>Choose Report</strong> window.</td>
<td><img src="image3.png" alt="Choose Report" /></td>
</tr>
<tr>
<td><strong>Tip</strong>  To create or edit reports, see <strong>Defining Reports (Report Manager)</strong>, page 11-25.</td>
<td></td>
</tr>
<tr>
<td>b. From the Report window, click <strong>Settings</strong> to open the <strong>Report Generation</strong> window.</td>
<td><img src="image4.png" alt="Report Generation" /></td>
</tr>
<tr>
<td>- <strong>Title</strong>: Enter a Title for the report.</td>
<td><img src="image5.png" alt="Report Generation" /></td>
</tr>
<tr>
<td>- <strong>Format</strong>: Select if the report should be in <strong>Record-style</strong> or <strong>Table-style</strong>.</td>
<td><img src="image6.png" alt="Report Generation" /></td>
</tr>
<tr>
<td>- <strong>Output</strong>: Select the type of file to output. For example: PDF document or Excel spreadsheet.</td>
<td><img src="image7.png" alt="Report Generation" /></td>
</tr>
<tr>
<td>- Click <strong>OK</strong> to close the <strong>Report Generation</strong> window.</td>
<td><img src="image8.png" alt="Report Generation" /></td>
</tr>
<tr>
<td>c. Click <strong>Save and Close</strong> to save the <strong>Action</strong> settings and close the <strong>Report</strong> window.</td>
<td><img src="image9.png" alt="Report Generation" /></td>
</tr>
<tr>
<td>d. Repeat these steps to create additional <strong>Actions</strong> for the automated rule, if necessary.</td>
<td><img src="image10.png" alt="Report Generation" /></td>
</tr>
</tbody>
</table>

**Step 7**  Select the Notification method. For example, send the report file by e-mail:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. From the Notification row, click the <strong>New</strong>... button. Notification options are: <strong>E-mail</strong>, <strong>FTP</strong> or <strong>Syslog</strong>.</td>
<td><img src="image11.png" alt="Select Notification Type" /></td>
</tr>
<tr>
<td>a. Select <strong>E-mail</strong> from the notification drop-down and configure valid e-mail addresses as displayed in the following step.</td>
<td><img src="image12.png" alt="Select Notification Type" /></td>
</tr>
<tr>
<td>b. Click <strong>OK</strong>.</td>
<td><img src="image13.png" alt="Select Notification Type" /></td>
</tr>
</tbody>
</table>
Step 8

a. Add e-mail addresses for the **To**, **CC**, and or **BCC** fields. You can enter specific e-mail addresses, or select addresses from the Personnel records configured in Cisco PAM.

b. Click **OK** to save the changes and close the window.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Add e-mail addresses for the <strong>To</strong>, <strong>CC</strong>, and or <strong>BCC</strong> fields.</td>
<td><img src="image" alt="E-mail Notification" /></td>
</tr>
<tr>
<td>b. Click <strong>OK</strong> to save the changes and close the window.</td>
<td></td>
</tr>
</tbody>
</table>
### Step 9

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Verify that all configurations are correct.</td>
<td><img src="image" alt="Edit - Automation Rule" /></td>
</tr>
<tr>
<td>b. Click <strong>Save and Close</strong> to save the Automated Rule and close the window.</td>
<td><img src="image" alt="Edit" /></td>
</tr>
</tbody>
</table>

### Step 10

Add the Automation driver as described in **Enabling the Automation Driver**, page 11-12.

**Note**  
This step is only necessary if the Automation Driver is not already added.
Defining Reports (Report Manager)

Use the Report Manager to add or modify reports used in automated tasks. Report templates include the following:

**Filter-based reports**
Reports defined using a filter, similar to the Filter toolbar button in many modules. This is the most straightforward way to define a report. For more complex reports, use one of the following SQL-based options.

**Object SQL-based reports**
Reports defined using explicit SQL which returns the unique IDs of the items to display, which are otherwise presented in a similar fashion as a filter-based report does.

**SQL-based reports**
Reports defined using explicit SQL.

Tip
See Configuring Global I/O Automated Rules, page 11-12 for instructions to assign reports to automated tasks.

This section includes the following information:

- Using the Report Manager, page 11-26
- Filter-based Report Template, page 11-27
- Object SQL-based Report Template, page 11-28
- SQL-Based Report Template, page 11-29
Using the Report Manager

**Step 1** Select **Report Manager** from the Reports menu. The main window appears, as shown in **Figure 11-1**.

**Figure 11-1** Report Manager Main Window

![Image of Report Manager Main Window]

**Note** Some reports are used for internal processes and cannot be used to generate reports. For example: **Badges-Unused**.

**Step 2** Use the toolbar to perform the following actions:

- **Add**: Add a new report or folder. The following options are available:
  - **Add Folder**: Adds a new folder for report organization.
- **Import**: Import a previously exported report or set of reports from XML.
Defining Reports (Report Manager)

- **Export...**: Export all reports to an XML file, which may be later imported on the same or another system.
- **Edit...**: Select a report and click **Edit...** to view and modify the details of the report. You can also double-click the report entry.
- **Delete**: Delete the report.
- **Run**: Run the report and open the contents of the report in a new window.

### Step 3

Edit the report using the description in the following sections:

- **Filter-based Report Template**, page 11-27
- **Object SQL-based Report Template**, page 11-28
- **SQL-Based Report Template**, page 11-29

---

**Filter-based Report Template**

When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

All report types include the following toolbar buttons:

- **Save and Close**: Save changes and close the report.
- **Run**: Run the report and open the contents of the report in a new window.
- **Export...**: Export the report to an XML file, which may be later imported on the same or another system.

**Figure 11-2** shows the detail window for a Filter-based Report Template. Complete the fields according to the descriptions in **Table 11-1**.

**Figure 11-2 Filter-based Report Template**

**Table 11-1 Filter-based Report Template Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the report.</td>
</tr>
<tr>
<td>Max results</td>
<td>The number of results displayed in the report. -1 is unlimited results.</td>
</tr>
<tr>
<td>Item type</td>
<td>The type of category to build the filter based report on.</td>
</tr>
<tr>
<td>Edit Filter...</td>
<td>Defines the filter, similar to filters available in the toolbar. See <strong>Using Filters</strong>, page 3-12.</td>
</tr>
</tbody>
</table>
When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

All report types include the following toolbar buttons:

- **Save and Close**: Save changes and close the report.
- **Run**: Run the report and open the contents of the report in a new window.
- **Export...**: Export the report to an XML file, which may be later imported on the same or another system.

**Figure 11-3** shows the detail window for a Object SQL-based Report Template. Complete the fields according to the descriptions in **Table 11-2**.

### Object SQL-based Report Template

When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

All report types include the following toolbar buttons:

- **Save and Close**: Save changes and close the report.
- **Run**: Run the report and open the contents of the report in a new window.
- **Export...**: Export the report to an XML file, which may be later imported on the same or another system.

**Figure 11-3** shows the detail window for a Object SQL-based Report Template. Complete the fields according to the descriptions in **Table 11-2**.

### Table 11-1 Filter-based Report Template Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Settings...</td>
<td>Report generation options, which are the same as when generating a report from one of the other modules. For more information see Creating Reports, page 3-10.</td>
</tr>
<tr>
<td>Variable Parameters...</td>
<td>Parameters the user is be prompted to provide when the report is run.</td>
</tr>
<tr>
<td>Edit Columns...</td>
<td>Select the columns used in the report. Use the <strong>Up</strong> and <strong>Down</strong> buttons to reorder the columns for the report.</td>
</tr>
</tbody>
</table>

### Object SQL-based Report Template

When you add or edit a report, the **Report Manager** detail window includes properties for the specific type of report.

All report types include the following toolbar buttons:

- **Save and Close**: Save changes and close the report.
- **Run**: Run the report and open the contents of the report in a new window.
- **Export...**: Export the report to an XML file, which may be later imported on the same or another system.

**Figure 11-3** shows the detail window for a Object SQL-based Report Template. Complete the fields according to the descriptions in **Table 11-2**.

### Table 11-2 Object SQL-based Report Template Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the report.</td>
</tr>
<tr>
<td>Max results</td>
<td>The number of results displayed in the report. -1 is unlimited results.</td>
</tr>
<tr>
<td>Item type</td>
<td>The type of category to build the object SQL-based report on.</td>
</tr>
<tr>
<td>SQL</td>
<td>The SQL query to be executed. The SQL defined should only return a single column, which is the unique id of an object matching the <strong>Item type</strong> drop-down menu.</td>
</tr>
</tbody>
</table>
Defining Reports (Report Manager)

When you add or edit a report, the Report Manager detail window includes properties for the specific type of report.

All report types include the following toolbar buttons:

- **Save and Close:** Save changes and close the report.
- **Run:** Run the report and open the contents of the report in a new window.
- **Export...:** Export the report to an XML file, which may be later imported on the same or another system.

Figure 11-4 shows the detail window for a SQL-based Report Template. Complete the fields according to the descriptions in Table 11-3.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the report.</td>
</tr>
<tr>
<td>Max results</td>
<td>The number of results displayed in the report. -1 is unlimited results.</td>
</tr>
<tr>
<td>Item type</td>
<td>The type of category to build the object SQL-based report on.</td>
</tr>
<tr>
<td>SQL</td>
<td>The SQL query to be executed. The SQL defined should only return a single column, which is the unique id of an object matching the <strong>Item type</strong> drop down menu.</td>
</tr>
</tbody>
</table>
Table 11-3   SQL-Based Report Template Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Settings...</td>
<td>Report generation options. For more information on report settings see Creating Reports, page 3-10).</td>
</tr>
<tr>
<td>Variable Parameters...</td>
<td>Parameters the user is prompted to provide when running the report. Variable parameters replace question marks in the SQL query, in order. The number of parameters must match the number of question marks in the query.</td>
</tr>
</tbody>
</table>
System Integration

This chapter describes how to integrate the Cisco PAM data and actions with enterprise or third-party systems.

Contents

- Configuring URL Actions, page 12-2
  - Creating or Modifying URL Actions, page 12-3
  - Creating Automated Rules for URL Actions, page 12-7
  - Viewing URL Events, Alarms, and Logs, page 12-10
- Synchronizing Data Using Enterprise Data Integration (EDI), page 12-14
  - Before You Begin, page 12-14
  - Installing the EDI Licence and Desktop Application, page 12-15
  - Creating Active Directory Database Integration Projects Using EDI Studio, page 12-17
  - Creating SQL and Oracle Database Integration Projects Using EDI Studio, page 12-26
  - Importing, Starting, and Monitoring EDI Projects in Cisco PAM, page 12-33
- Accessing the SQL Database, page 12-41

Note

See also the Cisco Physical Access Control API Reference Guide for information on Web Services support.
Configuring URL Actions

URL actions provide access control integration with Cisco and third-party products. For example, URL actions can trigger the following in other systems:

- **Energywise Integration**: a URL action can turn switch ports on or off, including any devices connected to those ports using Power-over-Ethernet (PoE). For example, when a user enters a building using a Cisco access control badge, the switch-powered equipment associated with that user can be turned on. When they exit the building, the equipment is turned off.

- **Camera integration**: a URL action can control the pan, tilt and zoom (PZT) functions of cameras associated with a device. For example, the camera can turn and zoom toward a door when badge is swiped at a door.

- **Digital media player (DMP) integration**: when a door event occurs, a URL action can display a custom HTML page on a DMP display.

To configure URL actions, select **URL Actions** from the Admin menu (Figure 12-1).

**Figure 12-1**  **URL Actions Main Window**

- Click **Preview** to view the URL for an action.
- Double-click an entry to view configuration settings.
- Select an entry and click **Invoke** to run a static action (Dynamic actions cannot be manually invoked).

See the following sections for instructions to create and automate URL actions:

- **Creating or Modifying URL Actions**, page 12-3
- **Creating Automated Rules for URL Actions**, page 12-7
- **Viewing URL Events, Alarms, and Logs**, page 12-10
# Creating or Modifying URL Actions

To add or modify URL actions, complete the following instructions:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Select <strong>URL Actions</strong> from the Admin menu.</td>
<td><img src="image1.png" alt="Admin Menu Display" /></td>
</tr>
</tbody>
</table>

**Step 2**  
Click **Add** to create a new action, or select an existing action and click **Edit**. 

![URL Actions Display](image2.png)
### Configuring URL Actions

#### Chapter 12      System Integration

#### Step 3
Enter the basic properties in the URL Action window:

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. <strong>Name</strong>: enter a descriptive name.</td>
<td><img src="image" alt="Edit - URL Action" /></td>
</tr>
<tr>
<td>b. <strong>Description</strong>: enter a short description of the rule.</td>
<td>Name: Shows Directory  Description: Displays a directory entry.</td>
</tr>
<tr>
<td>c. <strong>Post / Get</strong>: select the method the listening server will implement.</td>
<td>Method: Get / Post  Protocol: HTTP / HTTPS  URL base: <a href="http://172.16.0.1/login_url">http://172.16.0.1/login_url</a>  Enabled</td>
</tr>
<tr>
<td>d. <strong>Http /Https</strong>: Select the connection method. The Cisco PAM default for secure connections is the present a client certificate, and accept all secure certificates.</td>
<td>Additional Path  Parameters  Authentication</td>
</tr>
<tr>
<td>e. Enter the <strong>URL base</strong>. For example: <a href="http://www.cisco.com">http://www.cisco.com</a></td>
<td>Value:</td>
</tr>
<tr>
<td>f. Select <strong>Enabled</strong> to enable or disable the action.</td>
<td>Add</td>
</tr>
</tbody>
</table>

#### Notes Regarding Base URLs
Enter the URL exactly as it appears in the browser after URL encoding. Special characters in URLs, such as spaces, are replaced with the corresponding ASCII character when entered in a web browser. URLs in a browser first and then copy and paste the encoded URL in the **URL base** field.

For example: the URL http://www.yahoo.com?thread=Wall Street includes a space between Wall and Street. When entered in a web browser, the URL is converted to http://www.yahoo.com?thread=Wall%20Street.

Copy and paste this converted URL into the **URL base** field.
Step 4  
(Optional) Enter any additional URL paths. In the final URL, these values are separated from the base URL (and from each other) with a forward slash (/). The additional path value can be fixed text or an event attribute.

a. Select the **Additional Path** tab.

b. To enter a **Value**, select one of the following:
   - **Fixed**: enter the fixed text.
   - **Event attribute**: select an attribute from the drop-down menu.
   
   Attributes include: Unique Event ID, Event Type/LogCode, Event Source, Device Type, Device Address, Location Site, Location Campus, Location Building, Location Floor, Location Area Name, Location Sub Area Name, Location Fully Qualified Name, Priority, Badge ID, User ID, Personnel ID, Person's Name (Last, First), Credential Watch Level, and Associated Camera ID.

c. Click **Add**. The additional path appears in the list.

d. Repeat these steps to create additional paths, if necessary.

e. Click **Preview** to view the complete URL.

**Tip**  
Always preview the URL before saving the URL action. Any dynamic elements in the URL are displayed in brackets (<>), and are replaced by the corresponding event used at run time.

For example, enter `sample_action` in the Fixed field. Click **Add** to add it to the list, and then **Preview** to view the URL:

`http://www.cosco.com/sample_action`

Next, select the **Event attribute** button and select **Device Type** from the drop-down menu. Click **Preview** to view the new URL:

`http://www.cosco.com/sample_action/<Device Type>`
To do this | Use this display
---|---
*Step 5*  
(Optional) Enter the parameters used to construct the URL. URL parameters consist of a name and a value, and are separated from the URL with a question mark (?).

a. Select the **Parameters** tab.
b. Enter a **Name** for the parameter. The name is always fixed.
c. Select a **Value** option and enter one of the following. The value can be fixed or dynamic:
   - **Fixed**: enter the value text.
   - **Event attribute**: select an attribute from the drop-down menu. The parameter is captured from the specified event.
     - Attributes include: Unique Event ID, Event Type/LogCode, Event Source, Device Type, Device Address, Location Site, Location Campus, Location Building, Location Floor, Location Area Name, Location Sub Area Name, Location Fully Qualified Name, Priority, Badge ID, User ID, Personnel ID, Person’s Name (Last, First), Credential Watch Level, and Associated Camera ID.
   - **Complete event**: Available for *Post* actions only. The entire event information is included as an xml segment in the data posted to the URL.
d. Click **Add**. The parameter appears in the list.
e. Create additional parameters, if necessary. Parameters are separated in the URL with an ampersand (&).
f. Click **Preview** to view the complete URL.

In the following example, the Parameter entries are shown after the question mark, and are separated by an ampersand (&).

http://www.cisco.com/sample_value/ <Device Type>?Fixed_Text=text_sample&Event_Attr=<Device Address>
### Configuring URL Actions

#### Creating Automated Rules for URL Actions

Complete the following instructions to create a rule that automatically invokes a URL action based on a schedule or access control event. You can also create a rule that is manually triggered using a Quick Launch button or other method.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Global I/O from the Events &amp; Alarms menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image1.png" alt="Global I/O" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Click Add.</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image2.png" alt="Add" /></td>
<td></td>
</tr>
</tbody>
</table>
### To do this

**Step 3**

Enter a Name for the rule and select or deselect the Enabled checkbox.

![Edit Automation Rule](image1)

**Use this display**

### To do this

**Step 4**

Enter a trigger type for the rule.

Click **New** or **Edit** to define the Trigger Type. The choices are:

- **Event**: The rule is invoked when an event matching the defined filter occurs. Select Event and then click **Edit Filter** to define the filter.

- **Periodic** (time schedule): The rule is invoked according to a **Monthly**, **Weekly**, or **Daily** schedule. Select the day of week or day of month, if necessary, and the **Time of day** (in a 24-hour format).

- **Manual Only**: The rule is invoked manually. Create a Quick Launch button for the rule or right-click the Automation Driver to select the rule.

![Add Automation Rule](image2)

**Step 5**

Select a URL Action:

a. Click **Add** to add an action.

b. Select the Action type **URL Action**.

c. Select a URL Action from the drop-down menu.

d. (Optional) Click **New** or **Edit** to create or modify a URL action. Click **Preview** to view the URL for the action. See Configuring URL Actions, page 12-2 for more information.

e. Click **Save and Close**.

![Add URL Action](image3)
**Step 6** Specify a *Notification* option to define where the notification or report file is sent. The options are:

- **E-mail**: Sends the notification or report file to one or more e-mail addresses. To enable e-mail notifications, you must enter the SMTP server settings in the Automation driver. For instructions, see *Enabling the Automation Driver, page 11-12*.

- **FTP**: Sends the file to the specified FTP server.
  - **Host**: The FTP server IP address or name.
  - **Username**: Log in username required by the FTP server.
  - **Password**: Password to log in to the FTP server.
  - **Path**: Path on the FTP server where files should be uploaded.

- **Syslog**: Sends the notification or report to a Syslog.
  - **Host**: The Syslog server IP address or name.
  - **Facility**: The facility to use when recording the information to the Syslog.

**Step 7** Select the event options. These events occur when the rule is successfully invoked, or when rule options fail.

Click the check boxes to activate or deactivate the options:

- **Record event when rule invoked**: Each time the rule is invoked, record an event.
- **Record event when trigger fails**: Each time the trigger fails, record an event.
- **Record event when action fails**: Each time the action fails, record an event.
- **Record event when notification fails**: Each time the notification fails, record an event.

**Step 8** Click *Save and Close*.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> Specify a <em>Notification</em> option to define where the notification or report file is sent. The options are:</td>
<td>![Image of configuration options]</td>
</tr>
<tr>
<td><strong>Step 7</strong> Select the event options. These events occur when the rule is successfully invoked, or when rule options fail. Click the check boxes to activate or deactivate the options:</td>
<td>![Image of event options]</td>
</tr>
<tr>
<td><strong>Step 8</strong> Click <em>Save and Close</em>.</td>
<td></td>
</tr>
</tbody>
</table>
Viewing URL Events, Alarms, and Logs

An event is recorded each time a URL action is created or invoked. If a URL action fails, an alarm is recorded.

The URL Log in the Cisco PAM Server Administration utility also displays the output (HTTP response) from URL actions.

Examples of URL events, alarms, and log entries are shown in the following sections:

- Viewing URL Action Events, page 12-10
- Viewing Alarms for Failed URL Action, page 12-11
- Event and Alarm Response Codes for URL Actions, page 12-11
- Viewing Logs for URL Action Output, page 12-12
- URL Action Failure Due to Invalid Security Certificate, page 12-13

Viewing URL Action Events

To view events, select Events from the Events & Alarms menu, under the Monitoring sub-menu. Click the column titles to sort events by description, time, or other properties. Double-click the entry to view alarm details, or right-click an entry to select a command.

See Viewing Events, page 10-3 for more information.
Viewing Alarms for Failed URL Action

To view only failed URL actions, select Alarms from the Events & Alarms menu, under the Monitoring sub-menu. Use the Ack, Comment, and Clear buttons in the toolbar to clear the alarm or add comments. Double-click the entry to view alarm details, or right-click an entry and select a command.

See Viewing Alarms, page 10-8 for more information.

Event and Alarm Response Codes for URL Actions

The response code from the server is included in the data field. The response codes include the following:

**Event Response Codes**
- HTTP Status Code 200:OK
- HTTP Status Code 203:Non Authoritative
- HTTP Status Code 204:No Content
- HTTP Status Code 301:Moved Permanently
- HTTP Status Code 302 or 307:Temporary Redirect

**Alarm Response Codes**
- HTTP Status Code 400:Bad Request
- HTTP Status Code 401:Unauthorized
- HTTP Status Code 403:Forbidden
- HTTP Status Code 404:Not Found
- HTTP Status Code 405:Method Not Allowed
- HTTP Status Code 406:Not Acceptable
- HTTP Status Code HTTP Status Code 414:Request-URI Too Large
Configuring URL Actions

- HTTP Status Code 500: Internal Server Error
- HTTP Status Code 501: Not Implemented
- HTTP Status Code 503: Service Unavailable
- HTTP Status Code 505: HTTP Version Not Supported

Viewing Logs for URL Action Output

To display the output (HTTP response) from URL actions, open the URL Log in the Cisco PAM Server Administration utility.

**Step 1**
Log on to the Cisco PAM appliance as described in Logging on to the Cisco PAM Server Administration Utility, page 2-2.

**Step 2**
Select the **Monitoring** tab, and then select **URL Log**. Figure 12-4 shows the menu and sample log.

**Figure 12-4  URL Action Log**
URL Action Failure Due to Invalid Security Certificate

If a URL Action fails due to an invalid security certificate, the following log entry is displayed in the Cisco PAM Server Administration utility (see Viewing Logs for URL Action Output):

```
sun.security.validator.ValidatorException: PKIX path building failed:
  sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target.
```

To resolve this issue, do one of the following:

- When the URL Action was invoked by clicking the **Invoke** button in the URL Action window, restart the Cisco PAM client and try again.
- When the URL Action was invoked by an automated rule, stop and start the Cisco PAM server and try again. See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12 for instructions to restart the server.
- When the URL Action was invoked by a Quick Launch button, stop and start the Cisco PAM server and try again. See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12 for instructions to restart the server.
Synchronizing Data Using Enterprise Data Integration (EDI)

EDI is used to automatically synchronize records from an Active Directory personnel database to the Cisco PAM database. This section includes instructions to do the following:

- Install the **EDI license** on the Cisco PAM server.
- Download and install the **Cisco EDI Studio** desktop application on your PC.
- Use the EDI Studio to define integration projects, including the database connection, schema, and synchronization schedule.
- Import the data integration project file into Cisco PAM using the **EDI Administration** module.
- Monitor and troubleshoot data integration events using the **EDI Monitoring** and **Error Monitoring** modules.

Complete the following instructions to create, run, and monitor EDI integration projects:

- **Before You Begin**, page 12-14
- **Installing the EDI Licence and Desktop Application**, page 12-15
- **Creating Active Directory Database Integration Projects Using EDI Studio**, page 12-17
- **Creating SQL and Oracle Database Integration Projects Using EDI Studio**, page 12-26
- **Importing, Starting, and Monitoring EDI Projects in Cisco PAM**, page 12-33
  - **Importing and Starting EDI Projects**, page 12-33
  - **Verifying EDI Projects (EDI Monitoring)**, page 12-35
  - **Modifying a Running EDI Project**, page 12-37
  - **Restarting a Failed EDI Project**, page 12-39
  - **Summary of EDI Administration Functions**, page 12-39

Before You Begin

Review the following notes before creating EDI projects:

- This feature requires an optional Cisco license. The **EDI** menu appears only after the license is installed on the Cisco PAM server. See **Obtaining and Installing Optional Feature Licenses**, page 2-21 for instructions.
- The source database records are the master version: imported records cannot be deleted in Cisco PAM. Test a few personnel records in a staging environment before implementing EDI projects.
- Importing a large number of personnel records can cause system delays. To avoid system interruption, perform the initial import during off-peak hours, and stop the Gateway driver to allow the process to complete. To stop the driver, select **Hardware** from the **Doors** menu, right-click on the **Access GW Driver**, and select **Disable**. When the import is complete, select **Enable**. This process is only necessary when importing thousands of records, such as during the initial import of all database records.
- Personnel records are unique based on the ID number of the record. If a record is imported with the same ID number, then the current record is overwritten with the new data.
When organization and department values are included in an imported personnel record, those values must already exist in the Cisco PAM configuration. Before creating the EDI project, add the Organization values by manually creating them or through a data import. See **Editing Organization and Department Lists**, page 8-13 for more information.

All EDI projects run when the Cisco PAM appliance is stopped and restarted. If you do not want the projects to run after a server restart, stop the projects before restarting the server. See **Importing and Starting EDI Projects**, page 12-33.

EDI Active Directory (AD) projects run immediately when the camera driver is restarted, or when Cisco PAM is synchronized with the Cisco Video Surveillance Manager (Cisco VSM). The projects’ scheduled run time are also reset.

For example, if an AD project is scheduled to run at 5 pm daily, and the camera driver is restarted at 10 am, the EDI project will run and the schedule will be reset to 10 am. To avoid this, stop the EDI project before restarting the camera driver or synchronizing the Cisco VSM server. Restart the EDI project after the actions are complete. For more information, see **Summary of EDI Administration Functions**, page 12-39 and **Managing the Camera Inventory**, page 13-16.

Stop any running EDI projects before upgrading the Cisco PAM appliance software. After the upgrade, re-import the project to EDI Administration and start it again. See **Importing and Starting EDI Projects**, page 12-33 for instructions to stop, start and import EDI projects. If EDI projects are not stopped before a Cisco PAM upgrade, the project execution (or run) will not be successful. If this occurs, contact your Cisco support representative for assistance.

### Installing the EDI Licence and Desktop Application

To enable EDI database integration, complete the following tasks:

1. Install the EDI license on the Cisco PAM server.
2. Start the EDI driver in the Cisco PAM Hardware module.
3. Install the Cisco EDI Studio desktop software on your PC.

**Step 1** Install the EDI license on the Cisco PAM server. **Figure 12-5** Shows the EDI license installed on a Cisco PAM server. See **Obtaining and Installing Optional Feature Licenses**, page 2-21 for information to view the installed licenses or purchase and install new licenses.

**Figure 12-5**  
Cisco PAM Licenses

**Step 2** Create and start the EDI driver, if necessary.

a. Select **Hardware** from the Doors menu.

b. If the EDI Driver is included in the driver list, continue to **Step 3**.
c. If the EDI Driver is not included, right-click the **Driver Manager** and select **New EDI Driver**.

d. Right-click the EDI Driver and select **Start**. The driver status should be **Started** (see Figure 12-6).

**Figure 12-6  EDI Driver**

Download and install the EDI Studio desktop software.

a. Open a Web browser and enter the IP address for the Cisco PAM Server Administration utility.

b. Click **Download Cisco EDI Studio** on the Login page, as shown in Figure 12-7. You do not need to log on to the utility to download the software. The required version of Java is also installed, if necessary.

**Figure 12-7  Download EDI Studio**

Tip

You can also log in to the Cisco PAM Server Administration utility and select **Cisco EDI Studio (JRE Required)** from the Downloads menu. See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12.

c. Save the installation file to your local drive.

d. Double-click the EDI Studio installer file on your local drive to download and launch the installer.

e. Follow the on-screen prompts to install the EDI Studio desktop application. The application opens automatically when the installation is complete.
Creating Active Directory Database Integration Projects Using EDI Studio

The EDI desktop application is used to define data integration projects. Once created, the project is imported into the Cisco PAM to begin data synchronization.

This section provides an example to import personnel records from an Active Directory database into the Cisco PAM database. This example does not cover every possible scenario, and the specific records, fields and other data may not match the details for your site. Contact your Active Directory administrator for assistance when performing this process.

Review the following notes before creating and running an Active Directory project:

- Cisco PAM release 1.1 supports a single Active Directory project in EDI. You can create multiple AD projects, but only one can run.
- The Cisco EDI feature is tested and certified for Active Directory Server 2003.
- A user ID and password is required to access user objects from Active Directory schema.
- EDI supports photos in the JPEG format (the default is a maximum of 100kb per file).
- Users should not make major modifications to the Active Directory schema.
  - The User Object supports timestamp by default.
  - If changed timestamp is disabled in Active Directory, EDI project can not run.

Complete the following instructions to create a project for a Microsoft Active Directory database.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>Cisco EDI Studio</strong> on your Windows PC. The Cisco Enterprise Data Integration window opens.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a new Workspace.</td>
</tr>
<tr>
<td>a.</td>
<td>Select <strong>New Workspace</strong> from the File menu. You can also right-click <strong>Root</strong> and select <strong>New Workspace</strong>.</td>
</tr>
<tr>
<td>b.</td>
<td>Enter the Workspace name and click <strong>OK</strong>. The new Workspace is created along with a Projects folder.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td><strong>Root</strong> and <strong>Workspace</strong> help organize your projects. They do not serve any other purpose.</td>
</tr>
</tbody>
</table>
Chapter 12      System Integration

Synchronizing Data Using Enterprise Data Integration (EDI)

Step 3
Create a new EDI project.
Highlight the Projects folder and select New from the Project menu.
You can also right-click a Projects folder and select New.

Step 4
Name the project and enter the project properties:

a. **Project name**: enter the name of the project.
b. **Project template**: select a template for Microsoft Active Directory.
c. **Source DB**: select the source database.
d. **Destination DB**: select the destination database.
e. Click Next.

Step 5
Enter the Active Directory database parameters:

a. **Host name**: enter the IP address of the database server.
b. **Port**: enter the TCP port for the database server. Port 389 is the default for LDAP.
c. **Search base**: the Distinguished Name (DN) to use as a base for queries. For example: `dc=foobar`.

**Note** Cisco PAM is configured to send the `cn=` parameter, which must exactly match the `cn` parameter in Active Directory for the account.
d. **Login Name (Full DN)**: the username required to log in to the database.
e. **Password**: the database password.

**Note** The fields **Search base**, **Login name**, and **Password** are provided by your Active Directory administrator.
### To do this

**Step 6**

Click **Next** or **Test Connection** to validate the server settings.

- If the settings are valid, **Test connection successful** appears.
- If the settings are not valid, **Test connection failed** appears. One or more of the parameters is incorrect. Work with your Active Directory administrator to obtain the correct settings and test the connection again.

**Tip**

To verify the Active Directory user account attribute for the Cisco PAM login, use the tools described in the following step. Cisco PAM is configured to send the `cn=` parameter, which must exactly match the `cn` parameter in Active Directory for the account.

### Use this display

![Test connection successful](image1)

![Test connection failed](image2)
### To do this

**Step 7**

Map the equivalent fields between the *Destination Cisco PAM database* and the *Source AD attributes*.

- **a.** Enter the field name, or select an option from the drop-down menu.
  - Required destination fields are marked with an asterisk (*). The other fields are optional.
  - You must enter values for the **site** and **govt_id_spec**, either in this window, or in the following database properties window. If you enter values in the current window, the individual record data is used (and the default value is ignored). To use default values, leave the fields blank in this window and enter them in the following window (Default/Transform Values).
  - Select **userAccountControl** in the **emp_status** field to sync the AD account status attribute.
  - See also *Notes for Mapping the AD and Cisco PAM User Attribute Names*, page 12-21.

- **b.** Click **Next** to verify the settings and continue to the next configuration screen.
  
  Clicking next verifies the settings. If the test is not successful, verify that the prefix `cn=` is used for the login name in the Active Directory Source Parameters window, as described in **Step 5**.

**Tip**

If the test is not successful, verify that the prefix `cn=` is used for the login name in the Active Directory Source Parameters window (see **Step 5**).
### Notes for Mapping the AD and Cisco PAM User Attribute Names

In the AD structure, a user’s name includes an attribute `sn` for the last name, and another attribute `givenName` for the first name. For example: of Mike Smith would include:

- `sn=Smith`
- `givenName=Mike`

When you create an AD user log in for the Cisco PAM server, you must also configure a first and last name, or the database mapping will fail.

Two tools can help you determine the Active Directory attribute name that corresponds to a Cisco PAM record. The first is called **LDAP Browser/Editor**. Although Cisco does not provide this tool and does not document the tool usage, the sample output to the right shows the information you need to obtain for use with the EDI project. In this sample, the `cpam` user allows the Cisco PAM server to log in to the AD database. The `sn` attribute defines the lastname, and the `givenName` attribute defines the first name.

In addition, the Active Directory attribute `department` is defined. This attribute is mapped to the Cisco PAM field `govt_id`.

<table>
<thead>
<tr>
<th><strong>To do this</strong></th>
<th><strong>Use this display</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes for Mapping the AD and Cisco PAM User Attribute Names</td>
<td><img src="image" alt="LDAP Browser/Editor" /></td>
</tr>
</tbody>
</table>

To do this: Use this display

- In the AD structure, a user’s name includes an attribute `sn` for the last name, and another attribute `givenName` for the first name. For example: of Mike Smith would include:
  - `sn=Smith`
  - `givenName=Mike`

When you create an AD user log in for the Cisco PAM server, you must also configure a first and last name, or the database mapping will fail.

Two tools can help you determine the Active Directory attribute name that corresponds to a Cisco PAM record. The first is called **LDAP Browser/Editor**. Although Cisco does not provide this tool and does not document the tool usage, the sample output to the right shows the information you need to obtain for use with the EDI project. In this sample, the `cpam` user allows the Cisco PAM server to log in to the AD database. The `sn` attribute defines the lastname, and the `givenName` attribute defines the first name.

In addition, the Active Directory attribute `department` is defined. This attribute is mapped to the Cisco PAM field `govt_id`. | ![LDAP Browser/Editor](image) |
To do this

You can also extract user data to a CSV (comma separated value) file to view the Active Directory attributes.

For example the following command generates a CVS file with user data.

```
CSVDE -f onlyusers.csv -r "(&(objectClass=user)(objectCategory=person))"
```

This command runs the CSCDE (comma separated value data export) tool and creates a file named `onlyusers.csv`. Filters are used to limit the output to users and persons.

**Tip** Your system administrator may have additional knowledge of the CSVDE tool and output limiting filters.

Open the `onlyusers.csv` file in Excel to view the Active Directory attributes and the fields they map to, as shown in the Excel screen to the right. This screen shows how the fields correspond to the Cisco PAM personnel records fields.

The Cisco PAM Active Directory Personnel Data window is shown with the correct field mappings. Click Next to validate the attribute mappings.

---

**Step 8** Define the Active Directory default database values.

For example, enter the following in the in the **Source Attribute Value** column:

- **a.** Enter a **site**. The **site** must match the Cisco PAM site name. The site name is shown in the bottom right corner of all Cisco PAM client windows. The site name is also displayed at the top of the Hardware tree.

- **b.** Enter the **govt_id_spec** value.

**Note** The entries are ignored if values are also entered in the previous Personnel Data window. You must enter values for these fields in one of the windows.

- **c.** Enter the AD attribute for each of the **emp_status** fields. For example, `I` for inactive employees, `R` for retired employees, etc.

- **d.** Click **Next** to continue.
**Step 9**
(Optional) Select an EDI Extension file, if necessary.

EDI Extension files use API classes used to extend EDI functionality, including the following:

- Transform badge and personnel data received from an AD database. For example, remove the leading 1 from the Badge ID.
- Define default mapping. For example, assign Badge Templates based on the badge type.
- Provide cross field validation (such as dependency fields, correlation across different attributes or between badge and personnel data).

Extensions are built using a Cisco Systems framework and validated by the EDI Studio. Cisco also provides developer support.

**Procedure**

a. Click **Browse**.

b. Select the extension file that will be called when writing data into the personnel and badge interface tables. The extension file is validated by the EDI Studio.

c. Click **Next** to continue.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Select an EDI Extension file, if necessary.</td>
<td><img src="edi_extension.png" alt="Create New Project" /></td>
</tr>
<tr>
<td>EDI Extension files use API classes used to extend EDI functionality, including the following:</td>
<td></td>
</tr>
<tr>
<td>• Transform badge and personnel data received from an AD database. For example, remove the leading 1 from the Badge ID.</td>
<td></td>
</tr>
<tr>
<td>• Define default mapping. For example, assign Badge Templates based on the badge type.</td>
<td></td>
</tr>
<tr>
<td>• Provide cross field validation (such as dependency fields, correlation across different attributes or between badge and personnel data).</td>
<td></td>
</tr>
</tbody>
</table>
Synchronizing Data Using Enterprise Data Integration (EDI)

Step 10
Choose a schedule to specify how often data will be synchronized.

- **every hh:mm**: the data synchronization begins once every hour/minute specified.
- **every day**: the data synchronization is conducted once a day.
- **every week**: the data synchronization is conducted once a week.

**Scheduling Notes**

- Schedules are based on the Cisco PAM appliance time and time zone settings (not the AD source database server settings).
- The default project schedule is 60 minutes. This setting is configurable.
- The EDI (Core) frequency is two minutes. This setting is read-only.
- Cisco PAM retrieves records with a 15 minute overlap from the previous run to prevent loss of data; all records will be included even if the Cisco PAM and Active Directory server time settings are a few minutes apart.

Step 11
Click **Finish** to create the new database project and return to the main window.

The project is shown in the main window. A .jar file is saved to the following directory on your PC:

C:\Program Files\Cisco Systems\EDI Studio\workspaces\<Project_Folder>\projects

**Tip**
An error message appears if any fields are incorrect or missing. Use the **Back** button to navigate to the screen and correct the entry. When you are done, click **Finish** from the window the correction was made. You do not need to return to the last window. The entries in all windows are preserved.
### Step 12
(Optional) To change the data import rules or settings, select the project from the left window, and click **Edit** at the bottom of the detail window. Edit the settings as necessary and click **Save**.

**Tip** To change the name of a project, highlight the project and select **Rename** from the Edit menu. To delete a project, highlight the project and select **Delete** from the Edit menu.

### Step 13
Import the project in Cisco PAM and start the project to begin importing records.

See Importing, Starting, and Monitoring EDI Projects in Cisco PAM, page 12-33
Creating SQL and Oracle Database Integration Projects Using EDI Studio

Data projects define the source database connection and schedule information for an integration task. Once created, the project can be imported into the Cisco PAM EDI module to begin data synchronization.

This section provides an example to import personnel records into Cisco PAM from one of the following databases:

- MySQL version 5.0.4
- Oracle 10g versions.
- SqlServer 2005 and SqlServer 2000

This example does not cover every possible scenario, and the specific records, fields and other data may not match the details for your site. Contact your database administrator for assistance when performing this process.

Because SQL and Oracle projects are created for organization, personnel, and credential data, you must create separate projects for each data type, and run the projects separately. Each project must be monitored to ensure the data integration is complete and successful before the next project is started.

---

**Step 1**
Select Cisco EDI Studio on your Windows PC. The Cisco Enterprise Data Integration window opens, as shown in Figure 12-8.

**Figure 12-8  EDI Studio: Cisco Enterprise Data Integration Window**

---

**Step 2**
Create a new Workspace.
Figure 12-9   EDI Studio: New Workspace

a. Right-click Root and select New Workspace (or highlight Root and select New Workspace from the File menu).

b. Enter the Workspace name and click OK. The new Workspace is created along with a Projects folder.

Tip  Root and Workspace help organize your projects. They do not serve any other purpose.

Step 3  To create a new EDI project, right-click a Projects folder and select New (or highlight the folder and select New from the Project menu). The Choose Project Template window opens.

Figure 12-10   EDI Studio: New Project
Step 4  Select a Project Template, as shown in Figure 12-11.

Figure 12-11    EDI Studio: Choose Project Template

![EDI Studio: Choose Project Template](image)

- **Project name**: enter a name for the project.
- **Project template**: select a template that defines the data type (such as SQL credential data)
- **Source DB**: select the database source (such as Oracle or MySQL).
- **Destination DB**: select the destination database (SQL or MySQL).

**Note**
Oracle databases do not support boolean data types. You must define numeric data types and use them as boolean.

- Click **Next**.
**Step 5** Enter the source parameters, as shown in Figure 12-12.

*Figure 12-12  EDI Studio: Enter Parameters for the Source Database*

![EDI Studio: Enter Parameters for the Source Database](image)

- a. Enter the **Database name**.
- b. Enter the **User name** required to log in to the database.
- c. Enter the **Password** for the database password.
- d. Enter the **Server IP** address of the database server.
- e. Enter the TCP **Port** for the database server. Use a number between 1000 and 65536.
- f. Click **Next** or **Test Connection** to validate the server settings.
  - If the settings are valid, **Test connection successful** appears.
  - If the settings are not valid, **Test connection failed** appears. One or more of the parameters is incorrect. Work with your system administrator to obtain the correct settings and test the connection again.

**Step 6** Map the database fields for the Destination [Cisco PAM] database with the database fields for the Source database.

- a. Enter the **Source table name** of the source database.
- b. Enter a Source field for all required Destination [Cisco PAM] fields (marked with an asterisk*). The Destination fields are different for the type of data, as described in Table 12-1.
Table 12-1 shows the required fields for each data type:

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Required Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td><strong>Organization Data</strong></td>
</tr>
<tr>
<td></td>
<td>• name: (primary key) Name of the organization.</td>
</tr>
<tr>
<td>Department Data</td>
<td>• name: (primary key) Name of the department.</td>
</tr>
<tr>
<td></td>
<td>• orgName: (primary key) Organization name</td>
</tr>
<tr>
<td>Personnel</td>
<td>• site: Site of the personnel record.</td>
</tr>
<tr>
<td></td>
<td>• firs_name: User's first name.</td>
</tr>
<tr>
<td></td>
<td>• last_name: User’s last name</td>
</tr>
<tr>
<td></td>
<td>• govt_id: (primary key) Government ID number. If the govt_id is a social</td>
</tr>
<tr>
<td></td>
<td>security number, the length must be exactly nine digits. The valid values are:</td>
</tr>
<tr>
<td></td>
<td>I, II, III, Jr., and Sr.</td>
</tr>
<tr>
<td></td>
<td>• govt_id_spec: a unique id that can identify a personnel record. Valid values</td>
</tr>
<tr>
<td></td>
<td>are SSN, FIN, and ID#.</td>
</tr>
<tr>
<td></td>
<td>• emp_status: Employment status. The valid values are: active, inactive, on</td>
</tr>
<tr>
<td></td>
<td>leave, retired, and terminated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The emp_type is not required, but has the following valid values:</td>
</tr>
<tr>
<td></td>
<td>contractor, employee, employee_full_time, employee_part_time, intern, other,</td>
</tr>
<tr>
<td></td>
<td>vendor, and visitor. emp_type is a type of employee.</td>
</tr>
<tr>
<td>Credential (Badge Records)</td>
<td><strong>Note</strong> The Region and Nationality fields be values already defined in system.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The primary keys are badgeId and facilityCode.</td>
</tr>
<tr>
<td></td>
<td>• badgeId: (primary key) The badge ID.</td>
</tr>
<tr>
<td></td>
<td>• credTemplateId: Use this field to assign the parameters from a badge template</td>
</tr>
<tr>
<td></td>
<td>in Cisco PAM to imported badges. This option is used when importing badges</td>
</tr>
<tr>
<td></td>
<td>into Cisco PAM for the first time.</td>
</tr>
<tr>
<td></td>
<td>For example, create or edit a badge template in Cisco PAM as described in</td>
</tr>
<tr>
<td></td>
<td>Configuring Badge Templates, page 8-20. This template can contain settings for</td>
</tr>
<tr>
<td></td>
<td>fields such as access policy, facility code, badge type, watch level, and</td>
</tr>
<tr>
<td></td>
<td>effective date. Enter the name of the badge template in the Source Attribute</td>
</tr>
<tr>
<td></td>
<td>Value column for credTemplateId. For example: KeyPad_BCD4, 26BitWiegandCT,</td>
</tr>
<tr>
<td></td>
<td>26BitWiegandKeyPadCT, etc.</td>
</tr>
<tr>
<td></td>
<td>• facilityCode: (primary key) The facility code</td>
</tr>
<tr>
<td></td>
<td>• activationDate: Activation date for the badge.</td>
</tr>
<tr>
<td></td>
<td>• expirationDate: Date the badge expires. This date must be greater than the</td>
</tr>
<tr>
<td></td>
<td>activation date.</td>
</tr>
<tr>
<td></td>
<td>• validity: The valid values are: active, inactive, destroyed, lost, and stolen.</td>
</tr>
<tr>
<td></td>
<td>• role: The user’s role in the organization. The valid values are: employee,</td>
</tr>
<tr>
<td></td>
<td>contractor, vendor, and temporary.</td>
</tr>
</tbody>
</table>
c. **Source**: Enter the corresponding field name for the source database. Enter a name for all required Destination fields, and any additional fields, if necessary.

d. Click **Next**.

e. Organization data only: Enter the additional **Department Data** settings and click **Next** again.

**Step 7**
Define the default database values and click **Next** to continue.

**Step 8**
(Optional) Select an EDI Extension file, if necessary (**Figure 12-13**).

**Figure 12-13**  **EDI Studio: EDI Extension**

![EDI Studio: EDI Extension](image)

**Step 9**
Choose a schedule to specify how often data will be synchronized, as shown in **Figure 12-14**.

**Note**
EDI actions are conducted according to the Cisco PAM appliance time and time zone settings (not the source database server settings).

- **every hh:mm**: the data synchronization begins once every hour/minute specified.
- **every day**: the data synchronization is conducted once a day.
- **every week**: the data synchronization is conducted once a week.
Step 10  Click **Finish** to create the new database project and return to the Cisco Data Enterprise application window (Figure 12-8 on page 12-26).

The project is shown in the main window and the project file is saved to the default EDI project directory on your PC:

```
C:\Program Files\Cisco Systems\EDI Studio\workspaces\Project_Folder\projects\.
```

Tip  An error message appears if any fields are incorrect or missing. Use the **Back** button to navigate to the screen and correct the entry. When you are done, click **Finish** from the window the correction was made. You do not need to return to the last window. The entries in all windows are preserved.

Step 11  Import and start the EDI project in Cisco PAM.

See **Importing, Starting, and Monitoring EDI Projects in Cisco PAM**, page 12-33.
Importing, Starting, and Monitoring EDI Projects in Cisco PAM

This section includes the following information:

- Importing and Starting EDI Projects, page 12-33
- Verifying EDI Projects (EDI Monitoring), page 12-35
- Modifying a Running EDI Project, page 12-37
- Restarting a Failed EDI Project, page 12-39
- Summary of EDI Administration Functions, page 12-39

Importing and Starting EDI Projects

After the EDI projects are created, you must import the .jar project files into the Cisco PAM using the EDI Administration module.

To do this | Use this display
---|---
Step 1 Select **EDI Administration** from the **Admin** menu.

Step 2 Click **Upload** and select a project created using the EDI Desktop Studio.

The project .jar files are saved in the default EDI project directory on your PC:

C:\Program Files\Cisco Systems\EDI Studio\workspaces\<project_folder_name>\projects\
### Chapter 12  System Integration

#### Synchronizing Data Using Enterprise Data Integration (EDI)

<table>
<thead>
<tr>
<th>Step 3</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Once the file is uploaded, click <strong>Start</strong>.</td>
<td><img src="Image" alt="EDI Administration - Cisco Physical Access Manager" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Select the start time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Select <strong>Start Now</strong> (default) to run the project immediately.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Start Later</strong> to select a date and time to start the EDI project. The project will run at this time, and then at any scheduled time defined in the project file.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) You can also select a <strong>Data sync start time</strong> to perform the data synchronization from a particular date and time entered. Click the <strong>Data sync start time</strong> field to open a pop-up calendar. Double-click the date when the data sync should begin. The date and current time will be entered in the field. Edit the date and/or time if necessary.</td>
</tr>
</tbody>
</table>

**Note**  All EDI projects run when the Cisco PAM appliance is stopped and restarted. If you do not want the projects to run after a server restart, stop the project(s) before restarting the server.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Verify that the project is started.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="Image" alt="EDI Administration - Cisco Physical Access Manager" /></td>
</tr>
</tbody>
</table>
Verifying EDI Projects (EDI Monitoring)

Use the following information to verify that the record import is working.

**Step 1**  Select **EDI Monitoring** from the Admin menu to open the EDI Monitoring module (Figure 12-15).

![EDI Monitoring Menu](image)

The following information is displayed for each record

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The EDI event ID number.</td>
</tr>
<tr>
<td>Project Name</td>
<td>The name of the EDI project that the event as defined in the EDI Desktop Studio.</td>
</tr>
<tr>
<td>Project Type</td>
<td>The type of data, such as personnel, badge, or organization records.</td>
</tr>
<tr>
<td>Records Succeeded</td>
<td>The number of records successfully updated during the integration event.</td>
</tr>
<tr>
<td>Failed Records</td>
<td>The number of records that were not updated by the integration event. Failed record details are stored in the log files.</td>
</tr>
<tr>
<td>Extract Type</td>
<td>The type of data extraction including interface or core (see the following step).</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time when the data integration event began.</td>
</tr>
<tr>
<td>End Time</td>
<td>The date and time when the data integration event ended.</td>
</tr>
</tbody>
</table>

**Step 2**  Review the EDI projects on the EDI monitoring screen. There are two types of Extract Types (see Figure 12-16):

- **Interface:** this occurs when the Cisco PAM server connects to the Active Directory server and retrieves the records that have been added or modified since the last time the Interface extract was executed.

- **Core:** this occurs when the Cisco PAM server validates the records retrieved by the Interface process, and then edits the Cisco PAM personnel database to make the additions, deletions, or edits.
If the Interface entry shows success, but the Core does not, something in the extracted record is not compatible with the mapping between the Active Directory and Cisco PAM databases. For example, Figure 12-16 shows the following:

- ID 331 shows that the project imported 16 records from Active Directory.
- ID 341 shows that when we tried to update the Cisco PAM personnel records with the records extracted in 331, but something was wrong with the records, so all 16 failed.
- In ID 351 shows again that 16 records were extracted from the Active Directory.
- ID 361 shows that 3 of the 16 records were successfully added to the Cisco PAM personnel database.

**Step 3** To troubleshoot the errors and view additional error details, select **Error Monitoring** from the Admin menu (Figure 12-17).

**Step 4** The Error Monitoring window displays entries for each failed record, as shown in Figure 12-18. The Messages column includes text regarding the cause. For example: “Site is null” messages occur if the site name is not entered on the Default/Transform values screen of the EDI Studio project.
In addition, the following can occur:

Record updates in AD include a timestamp for the edit. When the Cisco PAM server connects, it compares the timestamp of the last edit in AD with what the last edit is that Cisco PAM knows about. If the AD timestamp is newer, the record is extracted.

Once the record is extracted from AD into Cisco PAM, the fields are checked for validity during the Core extract. For example if the AD last name (attribute \textit{sn}) contains a number, Cisco PAM should fail to import that record into the personnel database because a valid last name cannot contain a number.

\textbf{Step 5} Once the cause of the error is determined, modify the project. See \textit{Modifying a Running EDI Project, page 12-37}. If an EDI data integration project fails, identify and resolve the problem, and then complete the instructions in \textit{Restarting a Failed EDI Project, page 12-39}.

\section*{Modifying a Running EDI Project}

To modify an EDI project that is running, do the following:

\textbf{Step 1} Stop the project:
\begin{itemize}
  \item \textbf{a.} Select \textit{EDI Administration} from the \textit{Admin} menu.
  \item \textbf{b.} Select the project and click \textit{Stop}.
\end{itemize}

\textbf{Step 2} Click \textit{Export} to save the .jar project file. Save the file in the in the default EDI project directory on your PC:

\texttt{C:\Program Files\Cisco Systems\EDI Studio\workspaces\Project Folder\projects\}

\textbf{Step 3} Edit the project in EDI Studio:
\begin{itemize}
  \item \textbf{a.} Open the EDI Studio application on your PC.
  \item \textbf{b.} Select the project from the left window, and click \textit{Edit} at the bottom of the detail window.
  \item \textbf{c.} Edit the settings as necessary and click \textit{Save}.
\end{itemize}

\textbf{Tip} For field descriptions, refer to \textit{Creating Active Directory Database Integration Projects Using EDI Studio, page 12-17}. 
Step 4  Upload the modified project to Cisco PAM:
   a. Select EDI Administration from the Admin menu.
   b. Click Upload and select the .jar file that was saved in the default EDI project directory on your PC: C:\Program Files\Cisco Systems\EDI Studio\workspaces\<Project_Folder>\projects\.
   Note  Files can be saved to and uploaded from other locations.

Step 5  Select the project, click Start, and select the start time (Figure 12-20):

- Select Start Now (default) to run the project immediately.
- Select Start Later to select a date and time to start the EDI project. The project will run at this time, and then at any scheduled time defined in the project file.
• (Optional) You can also select a **Data sync start time** to perform the data synchronization from a particular date and time entered. Click the **Data sync start time** field to open a pop-up calendar. Double-click the date when the data sync should begin. The date and current time will be entered in the field. Edit the date and/or time if necessary.

---

**Restarting a Failed EDI Project**

If an EDI data integration project fails, identify and resolve the problem before restarting the project.

**Resolving Active Directory Issues**

If an error in the Active Directory record occurs, update the AD record. The EDI project will run according to the defined schedule. To force the project to run immediately, stop and then start the project. See **Summary of EDI Administration Functions, page 12-39**.

**Resolving Cisco PAM or EDI Studio Issues**

If an error occurs in the Cisco PAM database, do the following.

**Step 1** Correct the issue. For example:

- No organization values exist in the Cisco PAM records.
  When organization and department values are included in an imported personnel record, those values must already exist in the Cisco PAM configuration. Before creating the EDI project, add the Organization values by manually creating them or through a data import. See **Editing Organization and Department Lists, page 8-13** for more information.

- The project mapping is incorrect. See **Modifying a Running EDI Project, page 12-37** to correct mapping issues.

**Step 2** Delete the project in the EDI Administration.

a. Select **EDI Administration** from the **Admin** menu.

b. Select the project and click **Delete**.

**Step 3** Re-import and start the project. See **Importing and Starting EDI Projects, page 12-33**.

---

**Summary of EDI Administration Functions**

- **Column Descriptions**
- **EDI Administration Functions, page 12-40**

**Column Descriptions**

The EDI Administration window includes the following columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The data integration project name, as defined in the EDI Desktop Studio.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of data, such as personnel, badge, or organization records.</td>
</tr>
</tbody>
</table>
Synchronizing Data Using Enterprise Data Integration (EDI)

The following functions are available from the menu at the top of the project list:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refresh the window to display current information.</td>
</tr>
<tr>
<td>Upload</td>
<td>Upload a new or modified project from the EDI Desktop Studio. The project .jar files are saved in the default EDI project directory on your PC: C:\Program Files\Cisco Systems\EDI Studio\workspaces\Project_Folder\projects\</td>
</tr>
<tr>
<td>Export</td>
<td>Exports the project in the .jar file format.</td>
</tr>
<tr>
<td>Start</td>
<td>Runs a data integration project now, or at a specified time.</td>
</tr>
<tr>
<td>Tip</td>
<td>To create a recurring schedule for EDI projects, use EDI studio.</td>
</tr>
<tr>
<td>Note</td>
<td>All EDI projects also run when the Cisco PAM appliance is stopped and restarted. If you do not want the projects to run after a server restart, stop the project(s) before restarting the server.</td>
</tr>
<tr>
<td>Stop</td>
<td>Disables the project and stops data integration from running. A project cannot be stopped if currently running an integration. To update a project, you must first stop the project, modify it in EDI Studio, and then upload the revised .jar file. See c.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes the data integration project from Cisco PAM. The project remains in the EDI Desktop Studio.</td>
</tr>
</tbody>
</table>
Accessing the SQL Database

Use the command line to access the SQL database for personnel, time and attendance and user tracking data. Run the following file located on the Cisco PAM server:

/opt/cisco/cpam/import/MySQL_Views.sql

The username and password are:

- username: cpamuser1
- password: *******

Use the MySQL Query browser to view the following tables:

- Personnel, page 12-41
- Time and Attendance, page 12-42
- User Tracking, page 12-43

Personnel

The Personnel view (Figure 12-21) provides personnel information such as first name, last name, user id, personnel id, photo image, and the image type.

Figure 12-21 Personnel
Time and Attendance

The Time and Attendance view (Figure 12-22) provides information on user entry and exit through the Cisco Access Control Gateways. The information in this view includes first name, last name, personnel id, user id, door name, door location, reader name, entry or exit reader type, and the entry/exit time for the user.

You can optionally select all or partial data based on first name, last name, reader name, or a combination of these fields.

Figure 12-22 Time and Attendance
User Tracking

The User Tracking view (Figure 12-23) provides information regarding a user’s most recent use of the access control system, including the first name, last name, personnel id, user id, door name, door location, reader name, entry or exit reader type, and the door entry time.

You can optionally select all or partial data based on first name, last name, personnel id, or a combination of these fields.

Figure 12-23  User Tracking
CHAPTER 13

Video Monitoring

This chapter describes how to view live and recorded video streams from security cameras configured in the Cisco Video Surveillance Manager (Cisco VSM) system. Using Cisco PAM, you can associate these cameras with a door, and then view live and recorded video for that door. While viewing live video, you can also invoke a door command, or use the pan, tilt and zoom (PTZ) controls, if available on the camera.

For example, if an alarm occurs, you can view a recorded video clip when the alarm occurred, or open a live video stream for a camera associated with the door. Command options in the video player allow you to perform actions such as securing or opening the door.

In addition, the Camera Manager can display multiple live video streams in a grid arrangement, allowing a user to monitor multiple cameras at once.

Tip
- If a camera is deleted from the Cisco VSM configuration, it is disabled in Cisco PAM, but not removed. We recommend that you do not manually remove or delete cameras from the Cisco PAM configuration. Use the synchronize command to update the camera inventory, if necessary, as described in Managing the Camera Inventory, page 13-16.

- For more information on Cisco Video Surveillance Manager, go to the Cisco Network-Centric Video Surveillance Products website.

Note
Problems may occur when viewing video from analog cameras that use Cisco Stream Manager IP Gateway Encoder CIVS-SGxx. Contact your Cisco support representative for details.

Contents

- Enabling Video Monitoring, page 13-3
  - Configuring the Camera Driver, page 13-3
  - Associating Cameras with Doors and Devices, page 13-6
  - Installing the Cisco VSOM Video Client Desktop Application, page 13-8
- Viewing Video, page 13-9
  - Viewing Live Video in a Grid Arrangement, page 13-9
- Viewing Video for an Event, page 13-12
- Defining the Duration of Event Video Recording, page 13-15
- Managing the Camera Inventory, page 13-16
  - Updating the Camera Inventory, page 13-16
  - Deleting the Cisco VSM Cameras, page 13-18
  - Deleting Individual Cameras, page 13-22
- Recording Motion Events from Cisco VSM Cameras, page 13-24
Enabling Video Monitoring

To enable video viewing in Cisco PAM, add the camera driver and associate the Cisco VSM cameras with specific doors and devices.

In addition, install the Cisco VSOM Video Client on each workstation. This player includes the ActiveX controls required for event video viewing. Reinstall the player anytime the Cisco VSM server is upgraded.

Complete the following instructions to enable video monitoring:

- Configuring the Camera Driver, page 13-3
- Associating Cameras with Doors and Devices, page 13-6
- PC Workstation Requirements for Live Video Viewing, page 13-7
- Installing the Cisco VSOM Video Client Desktop Application, page 13-8

Configuring the Camera Driver

Add the VSM Camera Driver to enable video sharing and playback with the Cisco VSM system:

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><img src="image1" alt="Driver Manager" /></td>
</tr>
<tr>
<td>Select <strong>Hardware</strong> from the Doors menu.</td>
<td><strong>Hardware</strong> menu showing options such as Locations &amp; Doors, Templates, Access Policies, Schedule Manager, Device Status, Device IC Rules, Device Groups.</td>
</tr>
</tbody>
</table>

| **Step 2** | ![Driver Manager](image2) |
| Right-click the **Driver Manager** and select **New Cisco VSM Camera Driver**. | **Driver Manager** showing options such as Localhost - Access 6G Driver, Start All, Stop All, New Recent Events, New Automation Driver, New Historical Events Driver, New Web Services Driver, New Gateway Driver, New Logical Driver, New EDI Driver, New Cisco VSM Camera Driver. |
To do this | Use this display
---|---
**Step 3** Enter the driver name in the properties window. For example: Cisco VSM Camera Driver.  
**Note** Verify that the Enabled checkbox is selected (default).  
![Add Cisco VSM Camera Driver](image1)

**Step 4** Enter the camera Player Preferences:

- **Player width**: the width of the video player in pixels.
- **Player height**: the height of the video player in pixels.
- **Maximum player instances**: limits the number of simultaneous video players that can be open on the desktop at a time. Enter a number from 1 to 16. Enter a number at least three greater than the number of required screens. This allow pop-up video screens from critical alarms to display, such as from a duress alarm. See also PC Workstation Requirements for Live Video Viewing, page 13-7.
- **Position**: the position on the screen where the video player appears. If the position is set to **Center**, the video player opens in the center of the screen each time it is launched.

**Tip** The VSM Config tab displays VSM server settings. See **Step 7** to enter settings.

![Add - Cisco VSM Camera Driver](image2)

**Step 5** Click **Save and Close** to close the window.

![Save and Close](image3)

**Step 6** Right-click the VSM Camera Driver and select **Start** to enable the Cisco PAM video features.  
**Note** Verify that the driver status reads **Started**.

![Driver Status](image4)
**Chapter 13  Video Monitoring**

**Enabling Video Monitoring**

**Step 7**

Enter the Cisco VSM server settings.

**Note** Do not change the database name or port number once they are configured.

a. Right-click the **Cisco VSM Camera Driver** and select **Setup Cisco VSM**.

b. Enter the **Run Frequency (in minutes)**: the time between Cisco PAM / VSM synchronization. Cameras added or removed from Cisco VSM are updated in Cisco PAM. If the camera inventory changes often, enter a low number. If the inventory changes rarely, enter a high number. The default is 30 minutes.

c. Enter the **Database name**: the name of the Cisco VSM database. The default is `bas`.

d. Enter the **Server name**: the name or IP Address of the Cisco VSM database server.

e. Enter the **Port number**: the port number for the Cisco VSM database server. The default is `3306`.

f. Click **OK** to save the changes and close the window.

**Step 8**

Right-click the **VSM Camera Driver** and select **Synchronize with Cisco VSM** to populate Cisco PAM with the Cisco VSM cameras.

**Step 9**

Verify that the Cisco VSM cameras appear as children of the Camera Driver.

If the cameras do not appear, see **Updating the Camera Inventory, page 13-16**.

**Note** Cameras in Cisco PAM are organized in the same camera groups as Cisco VSM. In Cisco PAM, each camera can only appear in one group. In Cisco VSM, cameras can appear in multiple groups.

**Note** If a camera is deleted from the Cisco VSM configuration, it is disabled in Cisco PAM, but not removed. We recommend that you do not manually remove or delete cameras from the Cisco PAM configuration. Use the synchronize command to update the camera inventory.
## Associating Cameras with Doors and Devices

When a camera is associated with a door or device, you can view recorded video clips for the events that occur on that device, or open a live video stream for the camera from event entries. When viewing live video, you can also invoke commands for the door or device.

For example, if you assign a camera to the door configuration `Lab 1`, you can right-click an event for that door to view live or recorded video for that door.

To associate a camera with a door or device, do the following:

---

**To do this** | **Use this display**
--- | ---
**Step 1** Select Devices in Camera View from the Events & Alarms menu, in the Video sub-menu

**Step 2** Drag and drop the devices and doors from the left window pane to the cameras listed on the right.

You can associate cameras with more than one device, and devices can have more than one associated camera.

**Tip** Be sure to associate cameras only with devices that are in the camera’s view.

**Note** If the correct cameras do not appear, see Updating the Camera Inventory, page 13-16.
Enabling Video Monitoring

Tip
For more information about configuring Cisco VSM cameras, see the Cisco Video Surveillance Manager documentation.

PC Workstation Requirements for Live Video Viewing

PC workstations require the following features for proper operation with Cisco Video Surveillance Manager 4.0/6.0 or higher:

- **OS**: Windows XP Professional Service Pack 2
- **CPU**: Intel Core 2 Quad Q9650 – 3.0 GHz (HP xw4600 Workstation w/ 4 cores)
- **Memory**: 4GB DDR2 (3.5GB usable)
- **Graphics**: ATI 4850 512 MB
- **Cisco VSOM Configuration**: VMR mode enabled

### Tip
In the main Events window, you can display a Video column to signify if a camera is associated with a door or device. Click **Columns** in the menu bar, check the Video box and click **OK**. The Video column displays three dots if a camera is associated with the door or device.

### Step 3
(Optional) You can also associate cameras with devices by editing the camera properties.

- Double-click the camera in the Video or Hardware windows.
  The **Edit - Camera** window opens.
- Select the **Devices in View** tab.
- Check the devices to be associated with the camera.
  Associated cameras are listed in the far-right table.
- Click **Save and Close**.

### Step 4
(Optional) Exit and relaunch the CPAM client to ensure the camera associations appear correctly in the Events window.

**Tip**
For more information about configuring Cisco VSM cameras, see the Cisco Video Surveillance Manager documentation.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>(Optional) You can also associate cameras with devices by editing the camera properties.</td>
</tr>
<tr>
<td>a. Double-click the camera in the Video or Hardware windows.</td>
<td>The <strong>Edit - Camera</strong> window opens.</td>
</tr>
<tr>
<td>b. Select the <strong>Devices in View</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>c. Check the devices to be associated with the camera.</td>
<td>Associated cameras are listed in the far-right table.</td>
</tr>
<tr>
<td>d. Click <strong>Save and Close</strong>.</td>
<td><img src="image2.png" alt="Device Association" /></td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Exit and relaunch the CPAM client to ensure the camera associations appear correctly in the Events window.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> In the main Events window, you can display a Video column to signify if a camera is associated with a door or device. Click <strong>Columns</strong> in the menu bar, check the Video box and click <strong>OK</strong>. The Video column displays three dots if a camera is associated with the door or device.</td>
</tr>
</tbody>
</table>
Enabling Video Monitoring

- Browser: Microsoft Internet Explorer 6 or 7
- VSM 4.1/6.1.1 (Client version: 6.1.26.0)
- Gigabit Ethernet (GigE) network connection required

Installing the **Cisco VSOM Video Client Desktop Application**

The Cisco VSOM Video Client includes the ActiveX controls required for event video viewing. Install the player to enable the video features, or anytime the Cisco VSM server is upgraded. When the player is installed, any existing version is automatically deinstalled.

**Step 1** Verify that all PC workstations meet the [PC Workstation Requirements for Live Video Viewing](#), page 13-7.

**Step 2** Configure the VSM Camera Driver, as described in [Configuring the Camera Driver](#), page 13-3.

**Step 3** Highlight the **VSM Camera Driver**.

**Step 4** Click the **VSOM Video Client (install link)** to open the Cisco VSM download page in a web browser.

**Step 5** Enter the Cisco VSM username and password supplied by your systems administrator.

**Step 6** Click the link for the **VSOM Video Client**.

**Step 7** Follow the on-screen instructions to save the installation file to your local drive.

**Step 8** Double-click the installation file and follow the on-screen prompts to install the VSOM Video Client on your PC.
**Viewing Video**

You can view multiple live video streams in a grid arrangement, or view live and recorded video for an event. When viewing live video, you can invoke commands for the doors and devices associated with the camera.

**Tip**

You can also right-click the cameras listed under the VSM Camera Driver (in the Hardware module) and select **View Live Video**.

This section includes the following instructions:

- Viewing Live Video in a Grid Arrangement, page 13-9
- Viewing Video for an Event, page 13-12

**Viewing Live Video in a Grid Arrangement**

The Camera Manager allows you to view multiple video streams in a grid arrangement, and invoke commands for the devices associated with the cameras. For example, you can simultaneously monitor the video streams from four cameras, and manually trigger a command, such as *grant door access*, for a door associated with a camera.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select <strong>Camera Manager</strong> from the <strong>Events &amp; Alarms</strong> menu, in the <strong>Video</strong> sub-menu.</td>
<td></td>
</tr>
</tbody>
</table>

| Step 1 | Click the **Layouts** menu and select a layout that includes the number of cameras you want to view. |
To view video in Cisco Physical Access Manager:

### Step 1
(Optional) You can also select a pre-defined arrangement.

### Step 2
Select the cameras for viewing:

- **a.** Expand the hardware tree to locate a camera.
- **b.** Drag each camera icon onto a window pane to view live video from that camera.

**Tip** To remove the camera, click and drag the title bar of the camera screen off the grid.

### Step 3
(Optional) Invoke a command for a device associated with a camera.

For example, to deny access to a door.

- **a.** Click the **Device Commands** button to show (or hide) the command options.
- **b.** Select a **Device**.
- **c.** Select a **Command**.

**Tip** The commands are also available by right-clicking the camera name in the Hardware module.

- **d.** Click **Execute**.
- **e.** If additional options are available, select an option from the pop-up window and click **OK**.
### Chapter 13  Video Monitoring

#### Viewing Video

| Step 4 | (Optional) Operate the pan, tilt, and zoom (PTZ) camera controls, if available.  
| :--- |  
|  | - Click View PTZ to show (or hide) the controls. This option only appears for PTZ cameras.  
|  | - Use the arrows to pan and tilt the camera view. Use + and - to zoom.  
|  | - Select a PTZ preset from the Switch to drop-down menu.  
|  | ![View PTZ](image)

| Step 5 | (Optional) Save the camera view as an Arrangement.  
| :--- |  
| a. | Click Save or Save As to save the current camera layout as an Arrangement.  
| b. | Enter the arrangement name and click OK. The layout name appears in the window title bar.  
| ![Arrangement](image)

| Step 6 | (Optional) Create or modify additional arrangements using the menu bar controls:  
| :--- |  
|  | - Layout: selects a blank layout to display video from one or more cameras.  
|  | - Arrangement: selects a previously saved Arrangement of views and cameras.  
|  | - New: creates a new screen of views and cameras.  
|  | - Save: saves the current view as an Arrangement.  
|  | - Save As: saves the Arrangement under a different name.  
|  | - Delete: deletes the current layout.  
| ![Menu Bar](image)
Viewing Video

Viewing Video for an Event

If a device or door is associated with a camera, and an event occurs for that device, you can view a recorded video clip of the event. You can also view live video from the camera that captured the event.

To view the video for an event, use one of the following options:

- Open the event and click the Live Video or Event Video buttons for a camera.
- Right-click the event entry, select a camera from the menu, and select Live Video or Event Video.

**Note**

The video and camera options appear only if video is available for the event.

**Tip**

In the main Events window, you can display a Video column to signify if a camera is associated with a door or device. Click Columns in the menu bar, select Video, and click OK. The Video column displays three dots if a camera is associated with the door or device. To ensure the stars appear correctly, you must exit and relaunch the CPAM client after associating cameras with a device or door.

**To do this**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Events from the Events &amp; Alarms menu.</td>
<td><img src="image1.png" alt="Columns menu" /></td>
</tr>
</tbody>
</table>

**Step 2**

(Optional) In the main Events window, display the Video column to signify if a camera is associated with a door or device.

a. Click the Columns button in the menu bar.

b. Check the Video box.

c. Click OK.

d. In the main Events window, click the Video column header to sort the events and display the video events at the top of the list.

**Tip**

The Video column displays three dots if a camera is associated with the door or device.
Chapter 13  Video Monitoring

Viewing Video

To do this

Step 3
Select a video option from the right-click menu:

a. Right-click an event or alarm entry.

b. Select a camera from the command menu.

c. Select View Live Video or View Event Video.

Tip  The video and camera options appear only if video is available for that event.

Step 4  (Optional) You can also select the video options from the event detail window.

a. Double-click an event or alarm entry.

b. In the detail window, click View Live Video or View Event Video.

Tip  The video and camera options appear only if video is available for that event.

Step 5
When viewing recorded event video, use the controls under the video display to fast forward, rewind, pause, or play the clip.

Tip  Press the Rewind or Forward buttons multiple times to increase the speed. You can playback or rewind video at 1x, 2x, 3x, or 4x.
## To do this

When viewing live video, you can use the device commands for an associated device or door, or use the PTZ controls for the camera.

### Device Commands

a. Click **Device Commands** to show (or hide) the controls.
b. Select a device.
c. Select a command.
d. Click **Execute**.
e. If additional options are available, select an option from the pop-up window and click **OK**.

### PTZ Controls

Click **View PTZ** to show (or hide) the controls. This option only appears for PTZ cameras.

- Use the arrows to pan and tilt the camera view. Use + and - to zoom.
  - or
- Select a PTZ preset from the **Switch to** drop-down menu.
Defining the Duration of Event Video Recording

By default, event video is recorded for 5 seconds before the event occurs, and 5 seconds after the event occurs. To change the number of seconds event video is recorded, do the following:

**Step 1**  Select **System Configuration** from the Admin menu.
Select the Events/Alarms sub-menu.

![Figure 13-1 System Configuration Events/Alarm Window](image)

**Step 2**  Enter the following:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length of video to display pre-event</td>
<td>The number of seconds of video that are included before the event occurred.</td>
</tr>
<tr>
<td>Length of video to display post-event</td>
<td>The number of seconds of video that are included after an event occurs.</td>
</tr>
</tbody>
</table>

**Step 3**  Click **Save**.

**Step 4**  Restart the Cisco Physical Access Manager.

**Note**  Changes to system administration settings do not take effect until Cisco PAM is restarted.
Managing the Camera Inventory

- Updating the Camera Inventory, page 13-16
- Deleting the Cisco VSM Cameras, page 13-18
- Deleting Individual Cameras, page 13-22

Updating the Camera Inventory

The list of available Cisco VSM cameras is automatically updated as cameras are added or removed from the Cisco VSM system. In most situations, users do not need to update or manage the camera inventory. However, if the camera list is not accurate, do one of the following, in the order shown:

Tip

- Entering the **Restart**, **Setup VSOM**, or **Synchronize with Cisco VSM** commands will retrieve the camera inventory immediately, regardless of the configured run frequency. After the initial synchronization, the inventory is updated based on the scheduled run frequency.
- If a camera is deleted from the Cisco VSM configuration, it is disabled in Cisco PAM, but not removed. We recommend that you do not manually remove or delete cameras from the Cisco PAM configuration. Use the **Synchronize with Cisco VSM** command to update the camera inventory.

### To do this

- Revise the time span between automatic synchronization:
  - a. Right-click the **Cisco VSM Camera Driver** and select **Setup Cisco VSM**.
  - b. Enter the **Run Frequency (in minutes)**: this defines the time between synchronization. Cameras added or removed from Cisco VSM are updated in Cisco PAM. If the camera inventory changes often, enter a low number. If the inventory changes rarely, enter a high number. The default is 30 minutes.
  - c. Click **OK** to save the changes and close the window.
To do this

Right-click the **Cisco VSM Camera Driver** and select **Synchronize with Cisco VSM**.

This command manually synchronizes Cisco PAM with the Cisco VSM inventory.

If the camera inventory is still not correct, restart the camera driver: right-click the **Cisco VSM Camera Driver** and select **Restart**.

Verify that the driver reset was successful.

a. Select **Alarms** from the **Events & Alarms** menu, in the **Monitoring** menu.

b. Verify that the following three events are listed as succeeded:
   - archive data feed
   - live data feed
   - camera data feed

If the camera list is still not accurate, continue to the following section: **Deleting the Cisco VSM Cameras**.
Deleting the Cisco VSM Cameras

In some situations, the camera inventory may need to be deleted (for example, following a Cisco VSM server change). This is necessary only if the camera listing remains incorrect after completing the instructions in Updating the Camera Inventory, page 13-16.

If problems remain, select the camera driver command **Delete All Cameras**. This command deletes the Cisco PAM cameras and downloads a new, updated list from the Cisco VSM server.

Deleting the cameras does the following in Cisco PAM.

- Removes the Cisco VSM server configuration.
- Removes the history of all cameras from the Cisco PAM database.
- Deletes all events and audit records for the cameras.
- Deletes the entire camera inventory.

**Note** To successfully reset the camera database, you must remove all camera associating in the Camera Manager and Graphic Maps, as described in the following instructions.

To delete all cameras from Cisco PAM and reload the camera inventory from the Cisco VSM server, do the following:

---

### To do this

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Remove all camera references from the Camera Manager layout arrangements, and from any Graphic Map.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Select <strong>Camera Manager</strong> from the <strong>Events &amp; Alarms</strong> menu, in the <strong>Video</strong> sub-menu.</td>
</tr>
<tr>
<td>b.</td>
<td>Select each arrangement, and click and drag the title bar of each camera off the grid.</td>
</tr>
<tr>
<td>Tip</td>
<td>You can also delete the arrangement to remove the camera references.</td>
</tr>
<tr>
<td>c.</td>
<td>Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>d.</td>
<td>Select <strong>Graphic Map Editor</strong> from the <strong>Admin</strong> menu.</td>
</tr>
<tr>
<td>e.</td>
<td>Select any maps that include cameras.</td>
</tr>
<tr>
<td>f.</td>
<td>Right-click each camera icon and select <strong>Remove Device Icon</strong>.</td>
</tr>
<tr>
<td>Tip</td>
<td>You can also delete the entire map to remove the camera references.</td>
</tr>
<tr>
<td>g.</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

For more information, see the following:

- **Graphic Map Editor**, page 10-42.
## Managing the Camera Inventory

### Step 2
Enable the **Delete All Cameras** command and the **Allow deletion of devices with events** option in the System Configuration settings.

**Note** The **Delete All Cameras** command only appears after you enable it in the System Configuration window.

**Note** The **Delete All Cameras** command will fail to complete if you do not enable the **Allow deletion of devices with events** option.

1. Select **System Configuration** from the Admin menu.
2. Select the **Cisco Settings** sub-menu.
3. Select the check-box for **Display Delete All Cameras command on the camera driver**.
4. Select the **Miscellaneous** sub-menu.
5. Select the check-box for **Allow deletion of devices with events**. This allows cameras with associated events to be deleted from Cisco PAM.
6. Click **Save**.
7. To activate the change, stop and then restart the Cisco PAM server. See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12 for instructions.

### Step 3
Delete the cameras from Cisco PAM:

1. Open the Hardware module.
2. Right-click the Cisco VSM Camera Driver.
3. Select the **Delete All Cameras** command.
4. Click **OK** when the warning message appears. All events, alarms and audit messages for the cameras will be deleted.
### Chapter 13 Video Monitoring

#### Managing the Camera Inventory

<table>
<thead>
<tr>
<th>Step 4</th>
<th>To do this</th>
<th>Use this display</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the deletion was successful.</td>
<td><img src="image1.png" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>- If the action succeeds, all cameras are removed from the camera driver. An event is displayed: “Cisco VSM Camera Driver command Succeeded: Reset Cameras”. Continue to Step 5.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- If the action fails, some cameras are still displayed under the camera driver. If this occurs, do the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. View the event description to verify the issue. The event is: “Cisco VSM Camera Driver command failed: Reset Cameras”. Open the event to view the event Data. For example: “There was an error deleting camera(s). Please remove camera references if any from the graphic map editor and Camera manager layout arrangements.”</td>
<td><img src="image2.png" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>b. Locate and delete the remaining camera references from Camera Manager and the graphic maps (see Step 1).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Restart the camera driver to restore the full camera inventory (right-click the Cisco VSM Camera Driver and select Restart). The Delete All Cameras command only works when the complete inventory is present.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Invoke the Delete All Cameras command again, as described in Step 3.</td>
<td><img src="image3.png" alt="Image" /></td>
<td></td>
</tr>
</tbody>
</table>

| Step 5 | After the Delete Cameras command is successful, restart the camera driver: right-click the Cisco VSM Camera Driver and select Restart. | ![Image](image4.png) |
### Step 6

Verify that the driver reset was successful.

**a.** Select **Alarms** from the **Events & Alarms** menu, in the **Monitoring** menu.

**b.** Verify that the following three events are listed as succeeded:
- archive data feed
- live data feed
- camera data feed

---

<table>
<thead>
<tr>
<th>Event Date/Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/24/2009 19:38:00.000</td>
<td>Workstation Logged In</td>
</tr>
<tr>
<td>4/24/2009 19:39:09.000</td>
<td>Operator logged in</td>
</tr>
<tr>
<td>4/24/2009 19:33:09.000</td>
<td>Operator logged out</td>
</tr>
<tr>
<td>4/25/2009 19:30:00.000</td>
<td>Workstation Lograd Out</td>
</tr>
</tbody>
</table>
To delete individual cameras, do the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Remove the camera associations (for the camera to be deleted) from the Camera Manager arrangements, and from any Graphic Map.</th>
</tr>
</thead>
</table>

**Tip** You can also delete the entire camera arrangement or graphic map to remove the associations.

**Step 2** Enable the **Allow deletion of devices with events** option in the System Configuration settings.

**Step 3** (Optional) Right click the camera and select **Disable**. Cameras that were removed from Cisco VSM server are disabled by default. This command is only necessary if you want to remove a camera that is included in the Cisco VSM server inventory.

---

**Deleting Individual Cameras**

To delete individual cameras, do the following:

See Deleting the Cisco VSM Cameras, page 13-18 for information on a single command to delete all cameras.
Step 4 Select **All Devices** from the **Filter** menu to display the disabled device.

Step 5 Right click the camera and select **Delete**.

**Tip** If the camera is still associated with Camera Manager arrangements or graphic maps, an error message describes the location of the associations. Remove the associations and issue the **Delete** command again.

Step 6 Click **OK** to confirm that all associated events will be deleted.

**Note** See **Disabling or Deleting a Device or Door, page 6-19** for more information.
Recording Motion Events from Cisco VSM Cameras

This section includes instructions to record start motion and stop motion events for Cisco VSM cameras in Cisco PAM. When a motion event occurs, the system can optionally open a video pop-up window.

For more information about the Cisco Video Surveillance Operations Manager (Cisco VSOM) used to configure camera events, see the Cisco Video Surveillance Manager Software documentation.

Procedure

Step 1 Configure the Camera Driver as described in Configuring the Camera Driver, page 13-3. Skip to Step 2 if the camera driver is already configured.

Step 2 Install the optional API license on the Cisco PAM server.
- The API license allows Cisco VSM to post events to a Cisco PAM URL. If the optional API license is not installed, API requests to the Cisco PAM server return an error.
- To install the optional license, see the “Overview” chapter of the Cisco Physical Access Control API Reference Guide. See also the “Obtaining and Installing Optional Feature Licenses” section on page 2-21.
- Skip to Step 3 if the API license is already installed.

Step 3 Enable Cisco PAM Web Services:
Skip to Step 4 if Cisco PAM Web Services are already enabled.
- Log on to the Cisco PAM Server Administration utility, as described in the “Logging on to the Cisco PAM Server Administration Utility” section on page 2-2.
- Select the Monitoring tab and then select Status, as shown in Figure 13-2.

Figure 13-2 Services tab in the Cisco PAM Server Administration Utility

Note The Status window appears by default. This window also appears when you first log on.
c. Click the Enable button for Web Service API.
A confirmation message appears and the Status changes to Enabled.

Step 4 To record motion stop and start events, associate the camera to itself.

a. Select Devices in Camera View from the Events & Alarms menu, in the Video sub-menu, as shown in Figure 13-3.

Figure 13-3 Devices in Camera View Menu

b. Expand the Cisco VSM Camera Driver to display the available cameras, as shown in Figure 13-4.

Figure 13-4 Devices in Camera View: Camera to Camera Association

c. Drag and drop a camera from the left Devices pane to the same camera name in the right Cameras pane.
The camera is displayed as a child of the same camera.

Note If the correct cameras do not appear, see Updating the Camera Inventory, page 13-16.
Step 5  (Optional) To open a video pop-up window for door events, associate a door with the camera:

a. Expand the Logical Driver to display the configured doors, as shown in Figure 13-5.

Figure 13-5  Devices in Camera View: Door to Camera Association

b. Drag and drop a door from the left Devices pane to a camera in the right Cameras pane. The door is displayed as a child of the camera.

Step 6  Identify and record the Camera ID, as shown in Figure 13-6.

The Camera ID is used in the URL used to call the event, as described in Step 7.

a. Select Hardware from the Doors menu.
b. Expand the Camera Driver to display the available cameras.
c. Right-click a camera and select Edit from the drop-down menu.
d. Select the CameraConfig tab.
e. Record the number displayed in the Camera ID field.
Step 7 Add a URL Notification to the motion event using the Cisco Video Surveillance Operations Manager (Cisco VSOM) web-based software.

Note Only Cisco VSM events configured with URL notifications are sent to Cisco PAM.

a. Use a PC to log in to the Cisco VSOM web-based software:
   - Start Internet Explorer.
   - Enter the IP address or the host name of the server that is running Cisco VSOM.
   - Enter your username and password.
   - Click OK.
   - The VSOM Operator page appears (see Figure 13-7).

b. Click Admin to open the Administrator pages.

c. Click Event to open the event configuration page.

d. Create a new motion event, or edit an existing event, as described in the “System Management” chapter of the Cisco Video Surveillance Manager User Guide.

e. Select the Motion Start or Motion Stop tab for the event.
f. Select the Alerts tab.

g. Select the Enable URL Notification check box.

h. Enter the Cisco PAM URL for the motion event in the following format:

   \[ \text{http://cpam-ip-addr/acws/services/acvsm/recordCameraEvent?cameraId=number&eventType=type&eventTime=time_value} \]

   The URL includes the following parameters:
   
   - \text{cpam-ip-addr}: the IP address of the Cisco PAM server.
   - \text{number}: the \text{cameraId} number recorded in Step 6. For example: 65.
   - \text{type}: the \text{eventType}. For example: \text{CB.MOTION_START} or \text{CB_MOTION_STOP}
   - \text{time_value}: the \text{eventTime}. Enter a timestamp or 0 for the current time.

   In the following example, the Camera ID is 65, the Event Type records motion Start events, and the Event Time is “0”. An event time of “0” records events for the current time.

   \[ \text{http://10.10.10.2/acws/services/acvsm/recordCameraEvent?cameraId=65&eventType=CB.MOTION_START&eventTime=0} \]

i. Click Submit to save the changes.

---

Step 8

View the motion events in Cisco PAM Events:

a. Launch the Cisco PAM software and log in, if necessary.

b. Select Events from the Events & Alarms menu, under the Monitoring sub-menu.

c. Sort or search for the event, as described in the “Viewing Events” section on page 10-3.
Figure 13-8 shows an example of a **Camera Motion Start** event. Double-click the event entry for additional details.

**Figure 13-8    Camera Events in Cisco PAM**
CHAPTER 14

System Configuration Settings

This chapter describes the system-wide site settings available in the System Configuration module.

**Note** We recommend restricting access to the System Configuration module to administrators only. See Defining User Profiles for Desktop Application Access, page 4-2 for more information.

To modify the system configuration settings, do the following:

**Step 1** Select **System Configuration** from the Admin menu.

**Step 2** Select a configuration topic from the tabs on the left (Figure 14-1).

**Step 3** Enter the settings and configurations as described in the sub-sections listed below.

**Step 4** Click **Save** to save changes made in a system configuration window.

**Step 5** Restart the Cisco Physical Access Manager (exit and relaunch the application).

**Note** Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

Contents

- LDAP Settings, page 14-3
- Password Policy Settings, page 14-5
- Event/Alarms Settings, page 14-6
- Data Entry/Validation - Personnel Settings, page 14-7
- Data Entry/Validation - Badge Settings, page 14-8
- Custom Personnel Fields Settings, page 14-10
- Custom Device Fields Settings, page 14-11
- Custom Badge Fields, page 14-12
- Personnel ID Number Generator, page 14-13
Contents

- PIN Generator, page 14-14
- Card Number Generator, page 14-15
- Support Contact Information, page 14-16
- Badge Design, page 14-17
- Miscellaneous Settings, page 14-18
- Cisco Settings, page 14-20
LDAP Settings

The LDAP options (Figure 14-1) include login validation settings required to use the Lightweight Directory Access Protocol. See Table 14-1 for field descriptions.

Tip
For more information, see Configuring LDAP User Authentication, page 4-11.

Figure 14-1    LDAP Settings

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

- For Active Directory, the prefix should be the (uppercase) domain followed by \ (example: MY-DOMAIN\) and the suffix should be blank.
- For OpenLDAP, the prefix should be: uid=
  The suffix should be changed to reflect the actual domain.
  So for my-domain.com, this would be:
  ,dc=my-domain,dc=com

Table 14-1 describes the LDAP settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP</td>
<td>Click the checkbox to enable or disable LDAP support.</td>
</tr>
<tr>
<td>LDAP server URL</td>
<td>URL of LDAP server, must begin with ldap://</td>
</tr>
<tr>
<td></td>
<td>Example: ldap://192.168.1.1</td>
</tr>
<tr>
<td>Principle suffix</td>
<td>Appended to the username for authentication. See above.</td>
</tr>
<tr>
<td>Principle prefix</td>
<td>Prepended to the username for authentication. See above.</td>
</tr>
</tbody>
</table>
Chapter 14      System Configuration Settings

LDAP Settings

Note

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

Table 14-1   System Configuration LDAP Settings (continued)

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

Note
Password Policy Settings

The Password Policy options (Figure 14-2) determine password expiration and strength requirements.

Figure 14-2  Password Policy Settings

Table 14-2 describes the Password Policy settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords expire after (days)</td>
<td>Passwords expire after this many days.</td>
</tr>
<tr>
<td>Minimum alphabetic characters</td>
<td>Minimum number of a to z characters or A to Z characters in the password.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Minimum number of characters in the password.</td>
</tr>
<tr>
<td>Minimum uppercase characters</td>
<td>Minimum number of uppercase password characters.</td>
</tr>
<tr>
<td>Minimum lowercase characters</td>
<td>Minimum number of lowercase password characters.</td>
</tr>
<tr>
<td>Minimum numeric characters</td>
<td>Minimum number of numeric password characters.</td>
</tr>
<tr>
<td>Minimum special characters</td>
<td>Minimum number of special characters in the set specified below.</td>
</tr>
<tr>
<td>Set of “special” characters</td>
<td>Which characters qualify as special characters for the above.</td>
</tr>
</tbody>
</table>

Note

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Event/Alarms Settings

Use the Events/Alarms tab (Figure 14-3) to define how alarms are managed by the system, and how much video is recorded for events.

Figure 14-3   Events/Alarm Settings

Table 14-3 describes the Event and Alarms settings.

Table 14-3   System Configuration Alarm Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow commenting of cleared alarms</td>
<td>Allow operators to comment on alarms that have already been cleared.</td>
</tr>
<tr>
<td>Consolidate duplicate alarms window (mins)</td>
<td>If duplicate alarms are being consolidated, this is the maximum time difference between the original and the duplicate. If an alarm that would otherwise be considered a duplicate occurs after this time, it becomes a new original alarm and subsequent duplicate alarms will bump up its duplicate count.</td>
</tr>
<tr>
<td>Consolidate duplicate alarms</td>
<td>Consolidate duplicate alarms identical other than time, into a single alarm, with an increasing alarm count. This is useful for preventing a flood of individual alarms; for example, if an armed alarm point is on an external gate which is flapping in the wind, repeatedly triggering the alarm. It is not recommended that this be unchecked without careful consideration of the possible performance impact of the increased number of individual alarms.</td>
</tr>
<tr>
<td>Duplicate alarm cache size</td>
<td>The size of the cache for duplicate alarms.</td>
</tr>
<tr>
<td>Length of video to display pre-event</td>
<td>The number of seconds of video that are included before the event occurred.</td>
</tr>
<tr>
<td>Length of video to display post-event</td>
<td>The number of seconds of video that are included after an event occurs.</td>
</tr>
<tr>
<td>Repeat alert sounds</td>
<td>Defines if alarms sounds are played only once, or repeated.</td>
</tr>
</tbody>
</table>
Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

Data Entry/Validation - Personnel Settings

Figure 14-4 Personnel Data Entry Settings

Table 14-4 describes the Data Entry/Validation - Personnel settings.

Table 14-4 Data Entry/Validation - Personnel Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default personnel ID specifier</td>
<td>The type of personnel ID specifier the field will default to. The various ID specifiers will be available in the drop-down.</td>
</tr>
<tr>
<td>Allow duplicate personnel IDs</td>
<td>Allow personnel to be added with duplicate personnel IDs.</td>
</tr>
<tr>
<td>Warn about duplicate personnel IDs</td>
<td>Warn if personnel are added with duplicate personnel IDs.</td>
</tr>
<tr>
<td>Use signature capture</td>
<td>Enable the ability to capture personnel signatures with a signature capture device. Signature capture devices must be configured in the application preferences before they may be used. See Enabling Signature Capture Devices, page 8-45.</td>
</tr>
<tr>
<td>Use single-screen personnel wizard</td>
<td>Enables a single-screen personnel wizard used for personnel data entry. All personnel information is available on one screen.</td>
</tr>
</tbody>
</table>
Chapter 14      System Configuration Settings

**Data Entry/Validation - Badge Settings**

Note
Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

**Table 14-4    Data Entry/Validation - Personnel Settings (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use custom fields on personnel wizard</td>
<td>Enable custom fields in the single-screen personnel wizard. This makes the screen larger, but is useful if important data is being stored in the custom fields. Refer to custom fields in the Custom Personnel Fields window.</td>
</tr>
</tbody>
</table>

**Data Entry/Validation - Badge Settings**

**Figure 14-5    Badge Data Entry Settings**
Table 14-5 describes the Data Entry/Validation - Badge settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow printing of unsaved badges</td>
<td>Allows printing new badges before the badge is saved. For highest security, leave this unchecked. When allowed (which may be more convenient), it is possible to print a badge without having any record of the badge.</td>
</tr>
<tr>
<td>Set 'today' as the default effective date</td>
<td>Uses the current date as a new badge effective date.</td>
</tr>
<tr>
<td>Use single-screen badge wizard</td>
<td>Enables a single-screen badge wizard for data entry. Most badge properties are on one screen.</td>
</tr>
<tr>
<td>Require PIN to be unique</td>
<td>Requires cardholder PINs to be unique. Useful in systems that use PIN-only access-control.</td>
</tr>
<tr>
<td>Allow null PIN</td>
<td>Allows badges to have null PINs. Useful in systems that do not use PIN for access-control.</td>
</tr>
<tr>
<td>Require numeric hot stamp</td>
<td>Requires hot stamp field to be numeric.</td>
</tr>
<tr>
<td>Disallow leading zeros in hot stamp</td>
<td>Prohibits users from adding hot stamps with leading zeros.</td>
</tr>
<tr>
<td>Use effective times for badges</td>
<td>Select this checkbox to enable the effective time constraint for badges, in addition to effective date, which is always enabled.</td>
</tr>
<tr>
<td>Use expiration times for badges</td>
<td>Select this checkbox to enable the expiration time constraint for badges, in addition to effective date, which is always enabled.</td>
</tr>
<tr>
<td>Use custom fields on badge wizard</td>
<td>Enables custom fields in the badge wizard. This makes the screen larger, but is useful if important data is being stored in the custom fields.</td>
</tr>
<tr>
<td>Max PIN Length</td>
<td>The maximum number of characters in a PIN.</td>
</tr>
<tr>
<td>Disable batch badge printing</td>
<td>Enables or disables the batch printing module. See Printing Multiple Badges, page 8-36.</td>
</tr>
</tbody>
</table>

**Note**

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Custom Personnel Fields Settings

The Custom Personnel Fields defines the custom fields available in the personnel detail window.

Figure 14-6  Custom Personnel Fields

Table 14-6 describes the Custom Personnel Fields settings.

Table 14-6  Custom Personnel Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Personnel Field</td>
<td>Selects which of the available custom fields is to be viewed or edited.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the checkbox to enable the selected custom field.</td>
</tr>
<tr>
<td>Drop down</td>
<td>Select the checkbox to use a drop-down for entry the selected custom field.</td>
</tr>
<tr>
<td>Column header</td>
<td>Changes the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like the title of a book, for example: Driver's License Number.</td>
</tr>
<tr>
<td>Form label</td>
<td>Changes the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like a sentence, for example: Driver's license number.</td>
</tr>
</tbody>
</table>

Note
Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
## Custom Device Fields Settings

Configures which the custom fields which are available in the device detail window.

**Figure 14-7 Custom Device Fields**

Table 14-7 describes the Custom Device Fields settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Device Fields</td>
<td>Selects which of the available custom fields is to be viewed or edited.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the checkbox to enable the selected custom field.</td>
</tr>
<tr>
<td>Drop down</td>
<td>Select the checkbox to use a drop-down for entry the selected custom field.</td>
</tr>
<tr>
<td>Column header</td>
<td>Change the name of the column header of the selected custom field. The</td>
</tr>
<tr>
<td></td>
<td>column header is displayed in list view columns. To be consistent with the</td>
</tr>
<tr>
<td></td>
<td>rest of the application, this would be capitalized like the title of a book,</td>
</tr>
<tr>
<td></td>
<td>for example, Serial Number.</td>
</tr>
<tr>
<td>Form label</td>
<td>Change the name of the form label of the selected custom field. The</td>
</tr>
<tr>
<td></td>
<td>form label is displayed in detail window fields. To be consistent with the</td>
</tr>
<tr>
<td></td>
<td>rest of the application, this would be capitalized like the a sentence, for</td>
</tr>
<tr>
<td></td>
<td>example, Serial number.</td>
</tr>
</tbody>
</table>

**Note** Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Custom Badge Fields

Configures which the custom fields which are available in the badge detail window.

Figure 14-8  Custom Badge Settings

Table 14-8  Custom Badge Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Badge Fields</td>
<td>Selects which of the available custom fields is to be viewed or edited.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the checkbox to enable the selected custom field.</td>
</tr>
<tr>
<td>Drop down</td>
<td>Select the checkbox to use a drop-down for entry the selected custom field.</td>
</tr>
<tr>
<td>Column header</td>
<td>Changes the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like the title of a book, for example: Serial Number.</td>
</tr>
<tr>
<td>Form label</td>
<td>Changes the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like the a sentence, for example: Serial number.</td>
</tr>
</tbody>
</table>

Note

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Personnel ID Number Generator

The personnel ID number generator is used for generating random personnel ID numbers, and is useful when personnel IDs do not correspond to any pre-existing ID numbers, such as employee ID, Social Security Number.

**Figure 14-9  Personnel ID Number Generator Settings**

![System Configuration - Cisco Physical Access Manager](image)

**Table 14-9  Personnel ID Number Generator Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enables the personnel ID number generator. New personnel entries will have randomly generated ID numbers entered in the field.</td>
</tr>
<tr>
<td>Length</td>
<td>The digit length of generated IDs.</td>
</tr>
</tbody>
</table>

**Note**

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
PIN Generator

Use the PIN generator to generate random PIN numbers for badges.

Figure 14-10  PIN Generator Settings

![Figure 14-10 PIN Generator Settings](image)

Table 14-10  PIN Generator Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Present</td>
<td>Enable the personnel ID number generator. Adding new personnel will have randomly generated ID numbers entered in the field.</td>
</tr>
<tr>
<td>Length</td>
<td>The amount of digits in the generated PIN.</td>
</tr>
</tbody>
</table>

Note

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Card Number Generator

With the card encoder enabled the card number generator will create a card number with the minimum and maximum digits specified below.

**Figure 14-11  Card Number Generator Settings**

![Card Number Generator Settings](image)

**Table 14-11  Card Number Generator Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Present</td>
<td>Enables the card number generator. Adding new badges will have randomly generated card numbers entered in the Card # field.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Maximum amount of card digits.</td>
</tr>
<tr>
<td>Minimum</td>
<td>Minimum amount of card digits.</td>
</tr>
</tbody>
</table>

**Note** Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Support Contact Information

This information is displayed in the About window available from the Help menu. It is intended to be customized with the dealer/installer/integrator's contact information, as this is often the first contact for support purposes.

**Figure 14-12  Support Contact Information Settings**

![Support Contact Information Settings](image)

**Table 14-12  Support Contact Information Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>Support company's name.</td>
</tr>
<tr>
<td>Contact name</td>
<td>The name of the contact person.</td>
</tr>
<tr>
<td>Contact person's email address</td>
<td>The contact person's email address.</td>
</tr>
<tr>
<td>Contact person's phone number</td>
<td>The contact person's phone number.</td>
</tr>
<tr>
<td>Company's website</td>
<td>Support company's company website address.</td>
</tr>
</tbody>
</table>

**Note**

Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).
Badge Design

This window lists the database links available in **Badge Designer**.

**Figure 14-13  Badge Design Settings**
Miscellaneous Settings

This window includes a variety of settings, as described in Table 14-13.

Figure 14-14  Miscellaneous Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load all strings from database</td>
<td>Loads all text strings from the database. Used in conjunction with the advanced Text Strings module. Normally there is no reason to check this, as any strings that have been changed or customized since the time of install will be automatically loaded from the database.</td>
</tr>
<tr>
<td>Always open new modules in same window</td>
<td>If checked, opening a new module simply replaces the module in the same window, rather than opening a new window.</td>
</tr>
<tr>
<td>Enable Window&gt;New Window</td>
<td>Allows modules to be opened in multiple windows. Adds an additional New Window button to the toolbar.</td>
</tr>
<tr>
<td>Prevent force quit (Command-Q) on Mac OS X</td>
<td>Blocks the force quit command.</td>
</tr>
<tr>
<td>Allow deletion of items that normally may only be disabled</td>
<td>Enables a true delete option in some modules. Normally, important items should be disabled, not deleted. Even with this option enabled, only items that are not referenced by other items may be deleted. For example, if a device has an event occur for it, it may no longer be deleted, as the event references the device. This is because true deletion in this case would result in the inability to correctly report on any such events.</td>
</tr>
<tr>
<td>Allow deletion of devices with events</td>
<td>Deletes events associated with a device when a device is deleted. Note: Cisco recommends that you do not delete devices. Events that are associated with the device will be deleted if the device is deleted.</td>
</tr>
</tbody>
</table>
Chapter 14      System Configuration Settings

Note
Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

Table 14-13    Miscellaneous Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict new devices to wizards only</td>
<td>All new devices added to the <strong>Hardware</strong> module will use an add wizard.</td>
</tr>
<tr>
<td>Default max rows</td>
<td>Limits the number of visible rows in list-based modules such as Events and Badges. For example, if the default max rows is set to 100, the badges module displays a maximum of 100 rows. Enter a number between 1 and 5000.</td>
</tr>
<tr>
<td>Change queue buffer size</td>
<td>Enter a new buffer size.</td>
</tr>
<tr>
<td>Enable Credential Watch</td>
<td>Enables the Credential Watch feature which places color borders around photos in the Event Photos module. See <em>Adding a Color Border to Event Photos (Credential Watch)</em>, page 10-18.</td>
</tr>
<tr>
<td>Use cross-platform page setup dialog for badge printing</td>
<td>Select this option to use the cross-platform Java page dialog if the badge image is truncated. This occurs when using the default printer dialog on some printers (such as the Zebra printer).</td>
</tr>
<tr>
<td>Truncate imageable area values used to initialize cross-platform page dialog</td>
<td>If the image is still truncated using the cross-platform Java page dialog, select this option to apply .01 inch margins.</td>
</tr>
<tr>
<td>Use Pageable print interface for badge printing</td>
<td>The Java Printable printing interface is used by default. If printing problems occur (such as with the Evolis printer), select this option to use the Java Pageable printer interface.</td>
</tr>
<tr>
<td>Stroke text before printing badges</td>
<td>If problems occur printing text, such as on a Mac, select this option to apply a stroke when printing.</td>
</tr>
</tbody>
</table>
Cisco Settings

This window includes the settings described in Table 14-13.

**Figure 14-15   Cisco Settings**

![Cisco Settings](image)

You must restart the Cisco PAM appliance to activate changes made to all parameters in the *Cisco settings* screen except for **Display soft commands on default module** (this setting requires that you restart the Cisco PAM desktop application). See Performing Additional Configuration, Administration, and Monitoring Tasks, page 2-12, or ask your system administrator for assistance.

**Table 14-14   Cisco Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default discovered gateway time zone</td>
<td>Defines the time zone for all discovered Gateways. This time zone is configured on all discovered Gateways.</td>
</tr>
<tr>
<td>Credential download frequency (mins)</td>
<td>Defines how often (in minutes) credential information is downloaded to the Gateways. You can also download credential changes immediately. Select Hardware from the Doors menu, right-click on the Access GW Driver, and select Apply Credential Changes. See Configuring Personnel, page 8-2 for more information.</td>
</tr>
<tr>
<td>Display soft commands on default module</td>
<td>Displays the soft commands for the default m01 (Gateway) module.</td>
</tr>
<tr>
<td>Display “Delete All Cameras” command on the camera driver</td>
<td>Displays the Delete All Cameras command for the Cisco VSM Video Driver in the Hardware module. See Deleting the Cisco VSM Cameras, page 13-18.</td>
</tr>
</tbody>
</table>
Back up and Restoring Data

This appendix describes how to backup and restore the Cisco PAM database.

Create at least one data backup during the initial server configuration and after every upgrade. Data is backed up to a .zip file and automatically stored on the server disk drive. The file can also be downloaded to a workstation or network drive.

You can restore the data from a .zip archive only when the server is stopped.

**Note**

You must have at least one backup to restore the server software using the recovery CD. See Reinstalling the Cisco PAM Server Software from a Recovery CD, page B-14 for more information.

**Contents**

- Backing up the Cisco PAM Database, page A-2
- Archiving the Historical Events Database, page A-4
- Restoring a Server Backup File, page A-6
Back up the Cisco PAM Database

Use the Backup page to back up all Cisco PAM data and configurations, including live events and historical events. You can perform a one-time backup, or configure an automatic backup schedule. You can also copy the backup to a remote server.

Note

- In Cisco PAM release 1.2.0 and higher, data can be restored to a server with a different high-availability (HA) configuration. For example, data from a standalone server can be restored to a server in HA mode.
- To remove historical events from the main database and reduce the size of the backup file, complete the instructions in Archiving the Historical Events Database, page A-4.

To backup the Cisco PAM data and configurations, do the following:

**Step 1** Log on to the Cisco PAM appliance as described in Logging on to the Cisco PAM Server Administration Utility, page 2-2.

**Step 2** Select the Setup tab, and then select Backup, as shown in Figure A-1.

**Figure A-1** Backup Window in the Cisco PAM Server Administration Utility

**Step 3** Enter and re-enter the password for the backup file.

This password must be entered when the backup file is used to restore the system.

**Step 4** (Optional) Create an automatic backup schedule.

a. Check the Automatic Backup check box to display the Recurrence settings, as shown in Figure A-1.
b. Select the days when the backups will automatically occur:
   - To schedule backups for one day per month, select Date and then select a day of the month. For example: 15.
   - To schedule backups once per week, select Weekday and then select a day of the week. For example: Tuesday.
   - To run backups every day, select Daily.

c. Enter the Time when the automatic backups will run.
   Enter the time in 24 hour format (hh:mm:ss). For example, to run backups at 2 p.m., enter 14:00:00. To run backups at 1 a.m., enter 01:00:00.

d. Click Update to save the changes.

Step 5   (Optional) Automatically copy the backups to a remote server.

Use this option to automatically copy the backups to a remote FTP or SFTP server. The three most recent backups are also stored locally on the Cisco PAM server.

a. Check the Copy to remote server check box.
   The remote server settings appear, as shown in Figure A-1.

b. Select the server protocol:
   - SFTP: for secure file transfers using the Secure File Transfer Protocol (also known as the SSH File Transfer Protocol).

c. Enter the IP Address of the FTP or SFTP server.

d. Enter the Username for the FTP or SFTP server account.

e. Enter the Password for the FTP or SFTP server account.

f. Enter the directory Path on the for the FTP or SFTP server where the backup should be saved. The path must exist on the remote server. If the directory is not available, the backup will fail.

Note   If the IP address, username, password, or path is incorrect, or if the server is not available, then the backup is not copied to the remote server. The backup is still created on the Cisco PAM server.

Step 6   Click Backup Now to begin the backup process and create a new .zip backup file.

- If an automatic backup is scheduled, the backup will occur at the scheduled day(s) and time.
- When the backup is complete, the new backup file is added to the top of the screen, as shown in Figure A-1.
   - The file name includes the date and the server software version number. For example: December 16, 2009 11:53:15 AM PST.
   - The three most recent backup files are saved to the Cisco PAM server. When a new backup file is added, the oldest file is deleted.
   - To manually save the backup file to another location, right-click the filename and select a save option from the browser menu.
- If the backup is copied to a remote server, a copy of the file is saved to the server location configured in Step 5.
Archiving the Historical Events Database

When you copy and prune old events (as described in Archiving Historical Events, page 10-47) the events are moved to a separate Cisco PAM database. Although the events are no longer displayed in Events and Alarms, they are still included in the backup file (see Backing up the Cisco PAM Database, page A-2).

Archiving these historical events removes them from the database and saves them to a .zip file that can be saved to another location. The file includes a password-protected SQL script, and can be run on an offline database to view the purged events. Archiving historical events also improves system performance and reduces the size of the backup file.

Complete the following instructions to archive the historical events.

**Step 1** Copy and prune the events, as described in Archiving Historical Events, page 10-47.

**Step 2** Log on to the Cisco PAM appliance (see Logging on to the Cisco PAM Server Administration Utility, page 2-2).

**Step 3** Select the Setup tab, and then select Archive (Figure A-2).

**Step 4** Enter and re-enter the administrator password.
Step 5  Click the calendar icon to select the Archive Date & Time. Any events older than the selected date & time are included in the archive.

Step 6  Click **Start Archive** to begin the archive process and create a new .zip file. When complete, the new file is added to the top of the screen. The file name includes the Archive Date & Time.

For example: June 01, 2009 11:16:08 AM PDT.

Note  The three most recent archive files are saved. When a new archive file is added, the oldest file is deleted.

Step 7  To save the file to another location, right-click the filename and select a save option from the browser menu. The saved file includes the date (mm/dd/year), the Cisco PAM version number, and other information. The following file includes events from June 01, 2009 and earlier.

cpam-06012009-1116081.1.0_0.2.415.archive.zip
Restoring a Server Backup File

You can restore data from a backup file, or from an archive file.

**Before You Begin**

Note the following when restoring a backup or archive file:

- Data can be restored only when the server is stopped.
- Backup files include the Cisco PAM configuration and other data. See *Backing up the Cisco PAM Database, page A-2*.
- In Cisco PAM release 1.2.0 and higher, data can be restored to a server with a different high-availability (HA) configuration. For example, data from a standalone server can be restored to a server in HA mode.
- Archive files include only historical events that were removed from the database using the Archive function. Data is restored from an archive file so the historical events can be viewed using Cisco PAM events and reports. See *Archiving the Historical Events Database, page A-4* for more information.

**Procedure**

To restore the data from a backup or archive file, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that you have the correct backup file from either the Active or Standby server. See <em>Backing up the Cisco PAM Database, page A-2</em>.</td>
</tr>
<tr>
<td>2</td>
<td>Stop the Standby server, if installed.</td>
</tr>
</tbody>
</table>

**Note**

- For redundant HA configurations, ensure that both the Active and Standby servers are stopped (in **Down** state). Restoring a backup while either of the servers is up will result in unexpected behavior.
- If you are upgrading or reinstalling the server software, the Standby server should already be in the Down state.

a. Log on to the Standby Cisco PAM appliance.
b. Select the **Commands** tab, and then select **Stop Server**.
c. Select **Monitoring** and then select **Status**.
d. Verify that the Admin State is **Down**, as shown in Figure A-3.
Step 3  Stop the Active server.

Note

- For redundant HA configurations, ensure that both the Active and Standby servers are **Down** (Admin State). Restoring a backup while either of the servers is up will result in unexpected behavior.
- If you are upgrading or reinstalling the server software, the Standby server should already be in the Down state.

a. Log on to the Active Cisco PAM appliance.
b. Select the **Commands** tab, and then select **Stop Server**.
c. Select the **Monitoring** tab and then select **Status**.
d. Verify that the Admin State is **Down**, as shown in Figure A-3.

Step 4  On the Active server, select the **Setup** tab, and then select **Restore**, as shown in Figure A-4.
Restoring a Server Backup File

Step 5  Enter and re-enter the password for the backup file. This is the password entered when the backup file was created, as described in Backing up the Cisco PAM Database, page A-2.

Step 6  Click Browse to locate and select the .zip backup file.

Step 7  If the file is an archive file, select the Is Archived File checkbox.

See Archiving the Historical Events Database, page A-4 for more information.

Step 8  Click Restore.

Step 9  If restoring a backup file, wait for the Active server to automatically restart.

- A pop-up message appears informing you that the Web administrator utility is restarting.
- If the Cisco PAM Server Administration utility disconnects, a browser error message may be shown. Wait approximately five minutes for the server to restart, and then refresh your browser to log in again.

Step 10 Verify that the Active server is up.

a. Log on to the Active Cisco PAM appliance.

b. Select the Monitoring tab and then select Status, as shown in Figure A-5.

c. Verify the following:

- The Admin State is Up.
- The Server Mode is Active.

Figure A-5 Server Admin State (Up) for the Active Server

Step 11  Restart the Standby server, if installed.

a. Log on to the Standby Cisco PAM appliance.

b. Select the Commands tab, and then select Start Server.

c. Select the Monitoring tab and then select Status.

d. Verify the following:

- The Admin State is Up.
- The Server Mode is Standby.
Upgrading Software and Firmware

This appendix describes how to upgrade or reinstall the Cisco PAM server software, desktop client software, and Gateway module firmware.

Contents

- Upgrade Notes for Release 1.2.0, page B-2
- Obtaining Software Images and Other Tools, page B-5
- Obtaining Release Notes and Other Related Documentation, page B-5
- Upgrading the Cisco PAM Desktop Software, page B-6
- Upgrading the Cisco PAM Server Software, page B-7
- Upgrading to the Cisco Multi Services Platform (MSP) Appliance, page B-11
  - Replacing a Single (Non-Redundant) Server with an MSP, page B-11
  - Replacing Redundant HA Servers with MSPs, page B-11
- Reinstalling the Cisco PAM Server Software from a Recovery CD, page B-14
- Upgrading Gateway Firmware Images Using Cisco PAM, page B-18
  - Uploading Firmware Images to a TFTP Server, page B-18
  - Updating the Firmware on All Gateway Modules, page B-23
  - Updating the Firmware on Individual Gateway Modules, page B-28
Upgrade Notes for Release 1.2.0

- Credential Download Frequency Must be 60 Minutes or Higher, page B-2
- The Door Groups Feature Added to Device Groups, page B-2
- Enabling the Password Recovery Feature, page B-2
- Upgrading From Release 1.0.3 to Release 1.2.0, page B-3
- Split Holiday Schedule Configurations By Month, page B-3
- Select the Following Options When Upgrading Gateway Firmware, page B-3
- Generic Output Devices Installed Prior to Release 1.1.0 Must Be Rewired, page B-3
- Generic Output Device Command and Event Name Changes, page B-4
- Browser Time-out, page B-4
- Upgrade the Cisco PAM Desktop Client Software, page B-4
- Java Requirements, page B-4
- Stop EDI Projects Before Upgrading Cisco PAM, page B-5
- Change the Database Password Message, page B-5

Credential Download Frequency Must be 60 Minutes or Higher

The Credential download frequency cannot be set lower than 60 minutes. If a number less than 60 is entered, the setting will be reset to 60.

Note

The Credential download frequency defines how often (in minutes) credential information is downloaded to the Gateways.

To access the Credential download frequency setting, see Cisco Settings, page 14-20.

The Door Groups Feature Added to Device Groups

In Release 1.2.0 and higher, the Door Groups module is included in the Device Groups module. Any Door Group configurations from previous releases are automatically included in the Device Groups module following an upgrade.

Select Device Groups from the Doors menu to access the module.

Enabling the Password Recovery Feature

To enable the Cisco PAM Server Administration utility password recovery feature, the following fields must be configured (if not already set):

- Email Address
- SMTP Server Address
- SMTP Email Address from
See Enabling the Password Recovery Feature, page B-2 for instructions.

**Upgrading From Release 1.0.3 to Release 1.2.0**

To upgrade to Cisco PAM Release 1.2.0 from Release 1.0.3, you must first upgrade to Cisco PAM Release 1.1.0. For more information see the caveat CSCte56355.

**Split Holiday Schedule Configurations By Month**

Holiday schedules that span two months (for example, December 25 through January 4) do not operate correctly. Cisco PAM Release 1.2.0 prevents this configuration, and you must split the Holiday into two entries: one that covers the first month and the second that covers the following month.

For example, if a holiday schedule is required for December 25 through January 4, create one entry for December 25 through December 31, and a second entry for January 1 through January 4.

For more information, see the caveat CSCsq04020.

**Select the Following Options When Upgrading Gateway Firmware**

When upgrading Gateway firmware images to Cisco PAM Release 1.2.0 from any earlier release, select the following options:

- **Set as active image**: (checked by default) make the firmware file new active image.
- **Delete configuration**: delete the module configuration. The configuration is automatically reloaded when the module established communication with the Cisco PAM appliance.
- **Delete events**: delete all events stored on the module.
- **Reset Gateway**: (checked by default) perform a soft reset to powercycle the module. Changes to the active image are applied only after the Gateway is reset.

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

See the Upgrading Gateway Firmware Images Using Cisco PAM, page B-18 for instructions, or refer to the Cisco Physical Access Gateway User Guide.

**Generic Output Devices Installed Prior to Release 1.1.0 Must Be Rewired**

All Generic Output devices installed in Cisco PAM systems prior to release 1.1.0, were connected to the Gateway, Reader, or Output modules with the wiring reversed. In Cisco PAM release 1.1.0, the wires for these Output devices must be reinstalled to match the device manufactures recommended connections.

**Required Generic Output Device Connections in Cisco PAM release 1.1.0**

Disconnect all Generic Output devices installed with Cisco PAM release 1.0.0, 1.0.1, or 1.0.3, and do the following:

- Connect *Normally Open* devices to the N.O. and C connectors on the Gateway, Reader, or Output module.
• Connect Normally Closed devices to the N.C. and C connectors on the Gateway, Reader, or Output module.

Failure to re-wire these devices will cause the devices to act in the opposite way intended.

Generic Output Device Command and Event Name Changes

The following generic output device command names were changed for Release 1.1.0 and higher. The functionality is the same:

<table>
<thead>
<tr>
<th>Release 1.0.0 Command Name</th>
<th>Release 1.1.0 and Higher Command Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn output off</td>
<td>Activate Relay</td>
</tr>
<tr>
<td>Turn output on</td>
<td>Deactivate Relay</td>
</tr>
</tbody>
</table>

The following generic output device event names were changed for Release 1.1.0. The functionality is the same:

<table>
<thead>
<tr>
<th>Release 1.0.0 Event Name</th>
<th>Release 1.1.0 and Higher Event Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Off</td>
<td>Output Deactivated</td>
</tr>
<tr>
<td>Output On</td>
<td>Output Activated</td>
</tr>
</tbody>
</table>

Browser Time-out

When upgrading to Cisco PAM Release 1.2.0 and higher, the web browser may display an error such as “Page Not Found” while the upgrade is in process. Wait approximately five minutes for the upgrade to complete, then refresh the browser to display the login page.

Upgrade the Cisco PAM Desktop Client Software

Always upgrade the Cisco PAM desktop client when the server software is upgraded. If the versions are not the same, an error will occur when launching the desktop client. See Installing or Updating the Cisco PAM Desktop Software, page 3-2.

Java Requirements

Before upgrading the Cisco PAM server, upgrade your PC to Java 6.0 or higher (JDK 1.6 or higher), if necessary.

• To install Java 1.6, log on to the Cisco PAM appliance, select Downloads, and then select JRE 1.6 (Windows).
• To download the latest Java, go to http://www.java.com/en/download/manual.jsp
Stop EDI Projects Before Upgrading Cisco PAM

Stop any running EDI projects before upgrading the Cisco PAM appliance software. After the upgrade, re-import the project to EDI Administration and start it again. See Importing, Starting, and Monitoring EDI Projects in Cisco PAM, page 12-33 for instructions to stop, start and import EDI projects.

If EDI projects are not stopped before a Cisco PAM upgrade, the project execution (or run) will not be successful. If this occurs, contact your Cisco support representative for assistance.

Change the Database Password Message

When the server restarts, a message appears asking if you want to change the database password. Click Cancel or OK. This password is a security measure used for troubleshooting and technical support. It does not impact user operation.

Obtaining Software Images and Other Tools

To access the self-service portal and obtain software, documents, and tools, do the following:

1. Go to the following URL:
2. Click the Download Software link.
3. Log in to the Cisco Support Center. You must be a registered user of Cisco.com to access this page. You must have a current Cisco support contract that is linked to your Cisco.com account to download software and obtain help from the Cisco Technical Assistance Center.
4. Click the link for the correct release, or use the search function to locate the software release.

Tip
You can also log in to the Cisco Support Center at http://www.cisco.com/support/.

Obtaining Release Notes and Other Related Documentation

To obtain the latest documentation, including release notes, do the following:

Step 1
Go to one of the following URLs:
- Cisco Physical Access Manager Release Notes
- Cisco Physical Access Gateway Documentation
Upgrading the Cisco PAM Desktop Software

Always upgrade the Cisco PAM desktop client when the server software is upgraded. If the versions are not the same, an error will occur when launching the desktop client. See Installing or Updating the Cisco PAM Desktop Software, page 3-2 for instructions.
Upgrading the Cisco PAM Server Software

To upgrade the Cisco PAM server software, you must first stop the server. If you are upgrading redundant (HA) servers, you must stop both servers, upgrade the server that was originally designated as the Active server, and then upgrade the Standby server.

Before You Begin

- The following conditions apply when upgrading the Cisco PAM server software:
  - Upgrading either a single appliance or redundant servers causes system downtime. All servers must be placed in Down state to perform the upgrade.
  - System downtime can result in a temporary loss of data. Log and other system messages sent from the Cisco Physical Access Gateways and other hardware devices may be dropped during the upgrade process. Cisco recommends performing a manual upgrade only when system usage is low.
  - Software downgrades are not supported.
- Review the Upgrade Notes for Release 1.2.0, page B-2
- Obtain the correct software image. See Obtaining Software Images and Other Tools, page B-5.

Tip

The Cisco PAM server software is different from the desktop client software. The server software runs the appliance and provides a web administration interface used to configure and manage the server. The desktop (client) software runs on a PC and is used to configure devices and access control settings.

Procedure

To upgrade the Cisco PAM server software, do the following:

Step 1

Review the notes in Before You Begin.

Step 2

Backup either the Active or Standby server, as described in Backing up the Cisco PAM Database, page A-2. This backup is not required, but ensures the latest system data is preserved in case an error occurs.

Step 3

Stop the Standby server, if configured:

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

b. Click the Monitoring tab and verify the Server Mode is Standby (Figure B-1).

c. Select the Commands tab, and then select Stop Server.

d. Select the Monitoring tab and verify that the Admin State is Down.
Step 4  
Stop the Active server.

a. Log on to the Active appliance.

b. Click the Monitoring tab and verify the Server Mode is Active (Figure B-1).

c. Select the Commands tab, and then select Stop Server.

d. Verify that the Admin State is Down.

Step 5  
On the Active server, select the Setup tab, and then select Upgrade, as shown in Figure B-2.

Step 6  
Click Browse to locate and select the upgrade image.

Step 7  
Click the Upgrade button.

A pop-up message appears informing you that the Web administrator utility is restarting. If the Cisco PAM Server Administration utility disconnects, a browser error message may be shown. Wait approximately five minutes for the server to restart, and then refresh your browser.

Step 8  
Verify the upgrade process is complete, and the Active server is in Down state:

a. Log on to the Active Cisco PAM appliance.
b. Select the **Monitoring** tab and then select **Status**.

c. Verify the Server Version is correct. For example: 1.2.0

d. Verify the Admin State is **Down**.

e. Verify the Server Mode is **N/A**.

**Figure B-3 Server Admin State for the Active Server**

---

**Step 9** (HA configurations only) Upgrade the Standby server, if configured.

**Note** The Active server must be in **Down** state when you upgrade the Standby server, as described in **Step 8**. If a Standby server is not installed, skip to **Step 10**.

a. Log on to the Standby server.

b. Select the **Monitoring** tab and then select **Status**.

c. Verify that the Admin State is **Down**, as shown in **Figure B-3**

d. Select the **Setup** tab, and then select **Upgrade**.

e. Click **Browse** to locate and select the upgrade image, as shown in **Figure B-2 on page B-8**.

**f. Click Upgrade.**

**Note** Although the Standby server is upgraded, it is still in **Down** state. Start the Active server before starting the Standby server, as described in the following steps. Otherwise, the Standby server assume the Active role.

**Step 10** Restart the Active server.

a. Log on to the Active Cisco PAM appliance.

b. Select the **Commands** tab, and then select **Start Server**.

**Note** When the server restarts, a message appears asking if you want to change the database password. Click **Cancel** or **OK**. This password is a security measure used for troubleshooting and technical support. It does not impact user operation,
c. Select the **Monitoring** tab and then select **Status**, as shown in Figure B-4.

d. Verify the following:
   - Verify the Server Version is correct. For example: **1.2.0**
   - Verify the Admin State is **Up**.
   - Verify the Server Mode is **Active**.

*Figure B-4  Server Admin State (Up) for the Active Server*

<table>
<thead>
<tr>
<th>Cisco PAM Server Administration</th>
<th>Welcome</th>
<th>Log Out</th>
<th>About</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitoring</strong></td>
<td><strong>Status</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td><strong>Active</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Admin State:</strong></td>
<td><strong>Up</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Server Mode:</strong></td>
<td><strong>Active</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Server Version:</strong></td>
<td><strong>1.2.0</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Serial Number:</strong></td>
<td><strong>99291299990</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HA Availability Audit:</strong></td>
<td><strong>Enabled</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FTP Service</strong></td>
<td><strong>Up</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web Service API</strong></td>
<td><strong>Enabled</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 11**  (HA configurations only) Start the Standby server.

**Note**  Only start the Standby server after the Active server is Up, as described in **Step 10**.

a. Log on to the Active Cisco PAM appliance.

b. Select the **Commands** tab, and then select **Start Server**.

c. Click **Cancel** or **OK** for the database password message.

d. A pop-up message appears informing you that the Web administrator utility is restarting. If the Cisco PAM Server Administration utility disconnects, a browser error message may be shown. Wait approximately five minutes for the server to restart, and then refresh your browser.

e. Verify the upgrade was successful.
   - Log on to the Standby server.
   - Select the **Monitoring** tab and then select **Status**.
   - Verify the Server Version is correct. For example: **1.2.0**
   - Verify the Admin State is **Up**.
   - Verify the Server Mode is **Standby**.

**Step 12**  Upgrade the Cisco PAM desktop client, as described in **Installing or Updating the Cisco PAM Desktop Software, page 3-2**. If the versions are not the same, an error will occur when launching the desktop client.
Upgrading to the Cisco Multi Services Platform (MSP) Appliance

This section describes the process to replace an existing Cisco 1125 appliance with a Cisco Multi Services Platform (MSP) appliance.

Complete one of the following procedures:

- Replacing a Single (Non-Redundant) Server with an MSP, page B-11
- Replacing Redundant HA Servers with MSPs, page B-11

Replacing a Single (Non-Redundant) Server with an MSP

When replacing a single, non-redundant server, backup the system data from the old server immediately before bringing the new server online. You can only restore the data on the new server using the most recent backup: all data and configurations added to the system since the backup will be lost.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Backup the old server, as described in Backing up the Cisco PAM Database, page A-2. This backup is used to restore the system data to the new server.</td>
</tr>
<tr>
<td>2</td>
<td>Copy the backup file to a local disk, as described in Backing up the Cisco PAM Database, page A-2.</td>
</tr>
<tr>
<td>3</td>
<td>Physically install the new appliance, as described in the Cisco Physical Security Multi Services Platform User Guide.</td>
</tr>
<tr>
<td>4</td>
<td>Boot the new server and complete the instructions in Entering the Initial Server Configuration, page 2-4.</td>
</tr>
<tr>
<td>5</td>
<td>Restore the backup file to the new server, as described in Restoring a Server Backup File, page A-6.</td>
</tr>
</tbody>
</table>

Replacing Redundant HA Servers with MSPs

To replace one or both HA servers, complete the following tasks:

⚠️ Note This procedure results in system downtime.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Back up the Active or Standby server. The backup file is used to restore the system data on the new server.</td>
</tr>
<tr>
<td>a.</td>
<td>Log in to the Active or Standby appliance.</td>
</tr>
<tr>
<td>b.</td>
<td>Backup the system data, as described in Backing up the Cisco PAM Database, page A-2.</td>
</tr>
<tr>
<td>c.</td>
<td>Copy the backup file to a local disk.</td>
</tr>
</tbody>
</table>
Step 2  Stop the Active server.
   a. Log on to the Active appliance, as described in Logging on to the Cisco PAM Server Administration Utility, page 2-2.
   b. Select the Monitoring tab and then select Status.
   c. Verify the Server Mode is Active.
   d. Select the Commands tab, and then select Stop Server.
   e. Verify the following on the Monitoring > Status window, as shown in Figure B-5:
      – Verify the Admin State is Down.
      – Verify the Server Mode is N/A.

Figure B-5  Server in Admin State “Down”

Step 3  Stop the Standby server.

   Note  Stopping the Standby server results in system downtime since both servers are offline.

   a. Select the Commands tab, and then select Stop Server.
   b. Verify the Standby server is down in the Monitoring > Status window (Figure B-5):
      – Verify the Admin State is Down.
      – Verify the Server Mode is N/A.

Step 4  Physically remove the old servers and install the new Active and/or Standby servers, as described in the Cisco Physical Security Multi Services Platform User Guide.

Step 5  Boot the new Active appliance and complete the initial configuration, as described in Entering the Initial Server Configuration, page 2-4.
   • Be sure to follow the instructions for a Active server and enter the correct Shared IP address. See Understanding IP Addresses on the Cisco PAM Server, page 2-3.
   • You must obtain and install new Cisco PAM licenses, including the HA license. See Licensing: Frequently Asked Questions, page C-1 and Obtaining and Installing Optional Feature Licenses, page 2-21 for more information.

Step 6  Boot the new Standby appliance and complete the initial configuration, as described in Entering the Initial Server Configuration, page 2-4.
   • Be sure to follow the instructions for a Standby server and enter the correct Shared IP address.
You must reinstall the HA license on the Standby server. All other optional licenses are installed on the Active server only.

**Step 7** Verify that the redundant servers are in sync.

1. Log in to each server.
2. Open the Monitoring > Status window.
3. Verify that there are entries for Peer Address and Hostname, as shown in Figure B-6.

   If the HA servers are not in sync, the fields will be blank.

*Figure B-6  HA Status: Peer Address and Hostname*

**Step 8** Restore the backup file to the Active server, as described in Restoring a Server Backup File, page A-6.
Reinstalling the Cisco PAM Server Software from a Recovery CD

Use the recovery CD/DVD included with the Cisco PAM appliance to completely erase the server hard disk and re-install the Cisco PAM server software.

Caution
Reinstalling the server software from a CD/DVD using these instructions permanently erases all data and configurations on the Cisco PAM appliance. You must have at least one backup to restore the server software using the recovery CD. See Appendix A, “Backing Up and Restoring Data” for more information.

Note
To boot from the recovery CD/DVD, you must change the boot device order using the BIOS utility, as described in the following procedure.

Procedure

Step 1
Backup the data on your appliance. See Appendix A, “Backing Up and Restoring Data” for more information.

Tip
Backup and restore the server data to preserve critical system information and configurations.

Step 2
Insert the Cisco PAM recovery CD into the server DVD-ROM drive.

Step 3
Reboot the Cisco PAM appliance:

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

a. Select the Commands tab, and then select Reboot.

Step 4
Press and hold the Delete key while the appliance is restarting to open the BIOS setup utility, as shown in Figure B-7.
Step 5  Change the priority order of the boot devices so the CD/DVD drive is first boot priority, and the SCSI
hard drive is second priority.

Note  If you are using the Cisco Physical Access 1125 Appliance installed with Cisco PAM release
1.1.0 and earlier, you do not need to set the boot device using the BIOS setup utility. Skip to
Step 6.

a. Use the arrow keys to select the Boot menu, as shown in Figure B-8.

b. Select Boot Device Priority.
c. Use the arrow keys to select the **1st Boot Device**, and then press **Enter**.

A list of available devices appears, as shown in **Figure B-9**.

*Figure B-9  **Boot Device Priority Options***

![BIOS Setup Utility](image)

- **1st Boot Device**
- **2nd Boot Device**
- **3rd Boot Device**

**Options**
- **1st FLOPPY DRIVE**
- **USB-TEAC 00-205-01**
- **SCSI-DS68 05 0061L1 SW 01B**
- **Disabled**

**Figure B-10  **1st Boot Device = CD/DVD**

![BIOS Setup Utility](image)

- **1st Boot Device**
- **2nd Boot Device**
- **3rd Boot Device**

**Options**
- **STFC10 K185-00**
- **USB-TEAC 00-205-01**
- **SCSI-DS68 05 0061L1 SW 01B**
- **Disabled**

**d.** Use the arrow keys to select the CD/DVD device, and then press the **Enter** key.

**e.** Verify that the CD/DVD device is the **1st Boot Device**, and the SCSI hard drive is the **2nd Boot Device**, as shown in **Figure B-10**.

*Figure B-10  **1st Boot Device = CD/DVD***

![BIOS Setup Utility](image)

- **1st Boot Device**
- **2nd Boot Device**
- **3rd Boot Device**

**Options**
- **STFC10 K185-00**
- **USB-TEAC 00-205-01**
- **SCSI-DS68 05 0061L1 SW 01B**
- **Disabled**

**f.** Press the **F10** function key to save the changes and exit the BIOS utility.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>Wait for the CD to install the Cisco PAM server software. When finished, the server will reboot again.</td>
</tr>
<tr>
<td>Step 7</td>
<td>After the server reboots, remove the Cisco PAM recovery CD from the server DVD-ROM drive.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Configure the server as described in <em>Entering the Initial Server Configuration, page 2-4</em>.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Restore the system, as described in <em>Restoring a Server Backup File, page A-6</em>.</td>
</tr>
</tbody>
</table>
Upgrading Gateway Firmware Images Using Cisco PAM

The firmware image on all Gateways must be the same version as the Cisco PAM server software release. For example, if the Cisco PAM appliance is upgraded to release 1.2.0, then all Gateway modules must also be upgraded to firmware release 1.2.0. If the firmware release is different than the Cisco PAM appliance release, the Gateway will not operate and the Gateway status in the Cisco PAM Hardware module is **Mismatch**.

To ensure the Gateway firmware is the same release as the Cisco PAM appliance software version, complete the instructions in this section. You can upgrade all the Gateway modules at the same time, or individual Gateways.

Firmware images must be located on a TFTP server, such as the built-in Cisco PAM TFTP server). The firmware image file is then copied to the Gateway from the TFTP server. Since Gateways can store more than one firmware image, you must define which image is the active image, and then reset the Gateway module. When the module resets, the new firmware image is called the running image.

**Tip**

- To upgrade the firmware, activate a higher number release. To downgrade, activate a lower number release.
- You can also upgrade firmware using a PC directly connected to a Gateway module. See the *Cisco Physical Access Gateway User Guide* for more information.

This section includes the following information:

- Uploading Firmware Images to a TFTP Server, page B-18
- Updating the Firmware on All Gateway Modules, page B-23
- Updating the Firmware on Individual Gateway Modules, page B-28

Uploading Firmware Images to a TFTP Server

Firmware images used to update Gateway modules must be located on a TFTP server. You can load the images to the built-in Cisco PAM TFTP server, or to another TFTP server as described in this section.

Once the Firmware is copied to the TFTP server, you can load it to one or more Gateway modules, as described in Updating the Firmware on Individual Gateway Modules, page B-28 and Updating the Firmware on All Gateway Modules, page B-23.

**Tip**

You can use the built-in Cisco PAM TFTP server to store firmware images, or use a remote TFTP server. If using the built-in TFTP server, the server must be running. See Disabling the Cisco PAM TFTP Server, page D-2 for more information.

To load images to a TFTP server using Image Manager, do the following:

**Step 1** (Optional) Enable the built-in Cisco PAM TFTP server, if necessary.
Note

- The Cisco PAM TFTP server is enabled by default. Complete these steps only if the server was manually disabled, as described in Disabling the Cisco PAM TFTP Server, page D-2.
- If you are using firmware images located on another TFTP server (not the Cisco PAM server), skip to Step 2.

a. Log in to the Cisco PAM Server Administration utility.
   See Logging on to the Cisco PAM Server Administration Utility, page 2-2.
b. Select the Monitoring tab and then select Status, as shown in Figure B-11.
c. If the TFTP Service is Down, click Start.
d. Verify that the TFTP service is Up.

Figure B-11    TFTP Service in “Up” State

Step 2 Log in to the Cisco PAM desktop client.
   See Logging in to Cisco PAM, page 3-3.
Step 3 Select Image Manager from the Admin menu
   Figure B-12 shows the Image Manager window. Table B-1 on page B-20 describes each field.
Figure B-12  Image Manager

Table B-1  Image Manager Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 TFTP server</td>
<td>The IP address of the TFTP server to store image files.</td>
</tr>
<tr>
<td>2 Default</td>
<td>Click this button to IP address for the Cisco PAM TFTP server in the TFTP server field.</td>
</tr>
<tr>
<td>3 Remote Directory Path</td>
<td>The directory path on the TFTP server where files will be uploaded. The directory is in relation to the TFTP server root directory.</td>
</tr>
<tr>
<td></td>
<td>- If using the built-in Cisco PAM TFTP server, this field is read-only. Select the directory path using the Remote Browser.</td>
</tr>
<tr>
<td></td>
<td>- If using a TFTP server other than the built-in Cisco PAM server, this field is editable and you must enter the directory path on the TFTP server where files will be uploaded. The directory path must be valid since Cisco PAM does not validate remote server directories.</td>
</tr>
<tr>
<td></td>
<td>Note If this field is empty the image file is uploaded to the TFTP root directory. The default TFTP root directory is /tftpboot for Unix systems.</td>
</tr>
<tr>
<td>4 Remote Browser</td>
<td>Selects the directory where files will be uploaded on the build-in Cisco PAM TFTP server. This field is active only if you are using the build-in Cisco PAM server. Right-click within the field to display and select the following menu options:</td>
</tr>
<tr>
<td></td>
<td>- Create Directory: Creates a directory.</td>
</tr>
<tr>
<td></td>
<td>- Delete File/Directory: Enabled when a file or directory is selected. Deletes the file or directory</td>
</tr>
<tr>
<td>5 Download Button</td>
<td>Download a selected image on the TFTP server to the local drive.</td>
</tr>
</tbody>
</table>
Appendix B      Upgrading Software and Firmware

Upgrading Gateway Firmware Images Using Cisco PAM

Table B-1    Image Manager Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Upload Button</td>
<td>Uploads the selected image file to the specified TFTP server and directory. This button is enabled only when a file is selected in the Local directory browser.</td>
</tr>
<tr>
<td>7 Local Image Browser</td>
<td>The Local directory browser specifies the file on a local drive for upload to the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>• Click the Up button to navigate one level up.</td>
</tr>
<tr>
<td></td>
<td>• Double-click a folder to view the folder contents.</td>
</tr>
<tr>
<td></td>
<td>• Select a file to enter the file name and directory path in the Local Directory Path field and enable the Upload button.</td>
</tr>
<tr>
<td>8 Local Directory Path</td>
<td>Read-only. Displays the directory path and filename for the file selected in the Local browser. This file will be uploaded to the specified TFTP server.</td>
</tr>
</tbody>
</table>

Step 4  Upload firmware images to either the Cisco PAM TFTP server, or another TFTP server:

Uploading images to the Cisco PAM TFTP Server

a. Click Default to enter the Cisco PAM TFTP server IP address in the TFTP server field.

b. Select the file to be uploaded from the Local file browser. The selected file is automatically entered in the Local Image File field.

c. Use the Remote Browser to select the directory on the Cisco PAM TFTP server where files will be uploaded. This field is inactive if you are using a TFTP server other than the build-in Cisco PAM server.

Right-click within the Remote Browser to select the following menu options:

   – Create Directory: Creates a new directory on the Cisco PAM TFTP server.
   – Delete File/Directory: Deletes a selected file or directory.

d. Click Upload to add the file to the TFTP server specified in the TFTP server field.

Uploading Images to a Different TFTP Server (Not the Cisco PAM TFTP Server)

a. Enter the server IP address in the TFTP server field.

b. In the Remote Directory field, enter the TFTP server directory path where the image will be stored. If this field is left blank, then the root TFTP directory is used by default. The default Unix TFTP root directory is /tftpboot.

   Note  The TFTP server directory path entered in the Remote Directory field must be valid. Cisco PAM does not validate the existence of remote server directories.

c. In the Local file browser field, select the firmware file on a local drive to be uploaded. The directory path and filename are displayed in the Image File field.

d. Click Upload to add the file to the TFTP server specified in the TFTP server field.

Step 5  Continue to Updating the Firmware on Individual Gateway Modules, page B-28.
Tip

To download an image from the TFTP server to a local directory, select the image and local directory, then click the Download button.
## Upgrading the Firmware on All Gateway Modules

This section describes how to upgrade or downgrade all the Gateways configured in a Cisco PAM server.

### Tip

To upgrade the firmware for a single Gateway module, see Updating the Firmware on Individual Gateway Modules, page B-28.

### Before You Begin

Review the following before using the instructions to upgrading all Gateways.

- This procedure loads the same firmware image to all Gateway modules configured in Cisco PAM. If you check the options **Set as active image** and **Reset Gateway**, the Gateways will reset with the new image as the active *running* image.
- An *Active* image is the image that will be operational when the Gateway is reset. A *Running* image is the firmware image currently used to operate the Gateway.
- Gateways operate normally while the firmware image is being copied from the TFTP server, but are out of service while being reset. When a Gateway is down, the doors for that Gateway remain locked if the lock is fail-secure, and unlocked otherwise. See Understanding Door Modes, Door Schedules, and the First Unlock Feature, page 5-25 for more information.
- If you deselect the options **Set as active image** and **Reset Gateway**, then the firmware image is copied to the Gateways, but is not made the *Active* or *Running* image. You must use the File Manager to manually activate the image on each Gateway module, as described in Step 9, and then reset the Gateway as described in Step 10.
- Review the recommendations in Select the Following Options When Upgrading Gateway Firmware, page B-3.
- Gateways not configured in Cisco PAM are not impacted by this procedure.
- Gateways are upgraded in batches of 5, with a 15 minute delay between batches.
- 10 minutes after all the Gateways are updated, a summary event is posted to Cisco PAM. Any Gateways that are still in the Issued state are described as upgrade still in progress.
- You cannot issue another **Bulk Image Upgrade** command until the summary event is posted.

### Procedure

To upgrade or downgrade the firmware images for all Gateway modules, complete the following steps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Complete the instructions in Uploading Firmware Images to a TFTP Server, page B-18</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log in to the Cisco PAM desktop client. See Logging in to Cisco PAM, page 3-3.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Hardware</strong> from the <strong>Doors</strong> menu.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click the <strong>Access GW Driver</strong> and select <strong>Bulk Image Upgrade</strong> (Figure B-13).</td>
</tr>
</tbody>
</table>
Tip
You can also access the Bulk Image Upgrade command using the Locations & Doors module. Select Locations & Doors from the Doors menu, and then select Gateway Controllers from the View menu. Right-click a location or site and select Bulk Image Upgrade from the menu.

Step 5
In the Bulk Image Upgrade window (Figure B-14), enter the image location and select the upgrade options.

a. Enter the Image Name.
   - If the image is located on the Cisco PAM TFTP server, click Browse to select a firmware image name.
   - If the image is located on a different TFTP server, enter the filename manually.

b. Enter the TFTP Server IP address.
   The Cisco PAM appliance TFTP server IP address is entered by default.

c. Enter the directory Path on the TFTP server for the firmware image.
   - Leave this field blank if using the default location for the built-in Cisco PAM TFTP server.
   - Be sure the path and filename are valid. The administration tool does not verify remote server paths.

d. Select the following options to define what will occur after the image is loaded to the Gateway:
   - **Set as active image**: (checked by default) make the firmware file new Active image for all Gateways. The Active image is the firmware that will become the Running image when the Gateway is reset (see Figure B-18).
- **Delete configuration**: delete the module configuration on all Gateways. The configuration is automatically reloaded when the module establishes communication with the Cisco PAM appliance.

- **Delete events**: delete all events stored on all Gateways.

- **Reset Gateway**: perform a soft reset to powercycle all Gateways. Resetting the Gateway changes the Active image to the Running image. All Gateways will be down during the reset. Uncheck this box to reset the Gateways individually.

- **Reset time**: enter the time in 24-hour notation that the Gateways will begin to reset with the new firmware image. If this field is left blank, the Gateways will begin to reload in batches of 5 when you click **OK**.

**Note**  
See *Select the Following Options When Upgrading Gateway Firmware*, page B-3.

**Step 6**  
Click **OK** to close the window and begin copying the firmware image to the Gateway modules.

- Any actions selected in **Step 5d** are initiated. For example, the default option **Set as active image** makes the new image Active. The Gateways must still be reset for the image to become the Running image.

- Gateways are upgraded in batches of 5, with a 15 minute delay between batches.

- When all options are selected, wait an additional 10-15 minutes for the firmware upgrade to complete on each Gateway.

**Note**  
If you did not check the **Reset Gateway** option, the firmware image is copied to the Gateways and defined as Active, but is not made the Running image. See **Step 10** and **Step 9** to manually activate the image and reset each Gateway module.

**Step 7**  
Verify the upgrade status.

a. In the **Hardware** module, select the **Access GW Driver**.

b. In the **Extended Status** field for the driver, select the **Command Status** tab, as shown in **Figure B-15**.

c. Expand the **Bulk Image Upgrade** entry to view the upgrade status for each Gateway. The possible states include the following:
- **ISSUED**: The upgrade command was issued to the Gateway.
- **SUCCEEDED**: The Gateway image upgrade was successfully completed.
- **FAILED**: The Gateway image upgrade Failed for the reason in the description.
- **COMPLETED**: Cisco PAM cannot determine if the upgrade SUCCEEDED or FAILED. Completed indicates the command execution is complete, but you must manually verify the success or failure of the image upgrade using the File Manager.

**Note**
The status is shown as COMPLETED if the Gateway reboots, and the status is still ISSUED. This can happen if the Gateway has a large number of events in its queue when the module reboots, so the final status is not reported. Right-click the Gateway icon in the Hardware module and select **File Manager** to view the status of the loaded firmware images.

**Step 8** Review the summary event posted to the Cisco PAM Events module.

a. Select **Events** from the **Events & Alarms** menu, under the **Monitoring** sub-menu.

b. Double click the summary event to view details of the Bulk Image Upgrade, as shown in **Figure B-16**.

**Figure B-16 Summary Event for Bulk Upgrade Command**

- The summary event is posted 10 minutes after all the Gateways are updated.
- Any Gateways that are still in the **Issued** state are shown as **Upgrade in progress** in the Data field.
- You cannot issue another **Bulk Image Upgrade** command until all the summary event is posted.
Step 9 (Optional) Use the File Manager to verify the Active and Running firmware image for a Gateway module.

Tip
You can also change the Active image using the File Manager.

a. Right-click a Gateway Controller (blue icon) and select File Manager, as shown in Figure B-17.

Figure B-17 File Manager Menu

![File Manager Menu](image)

b. Select the Image tab to display a list of the firmware images currently loaded on the Gateway module, as shown in Figure B-18.

Figure B-18 File Manager Window: Image Tab

![File Manager Window: Image Tab](image)

Each row displays the following information about the firmware image:

- **Name**: the image filename.
- **Version**: the firmware version number.
- **Download Time**: the time and date when the image was downloaded to the Gateway module.
- **Active**: The Active image will become the Running image when the Gateway is reset. The image marked Yes is the active image on the Gateway.
- **Running**: The Running image is the image currently used to operate the Gateway. The image marked Yes is the current running image on the Gateway.

c. To change the active image, select an image name and click the Active Image button. This button is available only if the selected file is not the Active image.

d. To make the Active image the Running image, you must reset the Gateway. Right-click on the Gateway icon and select Reset Gateway, as described in Step 10.
e. Click **Close** to accept the changes and close the window.

**Step 10** (Optional) Reset individual Gateways.

This step is necessary if you did not select the option to **Reset Gateway** in Step 5d. The *Active* image becomes the *Running* image only after the Gateway is reset.

To reset the Gateway, do the following:

a. In the **Hardware** module, right-click a Gateway controller (blue icon).

b. Select **Reset Gateway**, as shown in Figure B-19.

![Figure B-19 Reset Gateway Command](image)

---

### Updating the Firmware on Individual Gateway Modules

You can load more than one firmware image to a Gateway module, and then upgrade or downgrade the firmware by selecting the *active* image and resetting the Gateway. Select a higher release to upgrade the firmware, or a lower release to downgrade.

**Note**

This section includes instructions for individual Gateways. To upgrade the firmware for all Gateways, see **Updating the Firmware on All Gateway Modules**, page B-23.

---

#### Before You Begin

Review the following before using the instructions to upgrading an individual Gateway.

- This procedure loads the same firmware image to all Gateway modules configured in Cisco PAM. If you check the options **Set as active image** and **Reset Gateway**, the Gateways will reset with the new image as the active *running* image.

- An *Active* image is the image that will be operational when the Gateway is reset. A *Running* image is the firmware image currently used to operate the Gateway.

- Gateways operate normally while the firmware image is being copied from the TFTP server, but are out of service while being reset. When a Gateway is down, the doors for that Gateway remain locked if the lock is fail-secure, and unlocked otherwise. See **Understanding Door Modes, Door Schedules, and the First Unlock Feature**, page 5-25 for more information.

- If you deselect the options **Set as active image** and **Reset Gateway**, then the firmware image is copied to the Gateway, but is not made the *Active* or *Running* image. You must use the File Manager to manually activate the image on each Gateway module, as described in Step 8, and then reset the Gateway, as described in Step 9.
• Review the recommendations in Select the Following Options When Upgrading Gateway Firmware, page B-3.

Procedure

Step 1 Complete the instructions in Uploading Firmware Images to a TFTP Server, page B-18

Step 2 Log in to the Cisco PAM desktop client. See Logging in to Cisco PAM, page 3-3.

Step 3 Select Hardware from the Doors menu.

Step 4 Right-click a Gateway Controller (blue icon) and select File Manager (Figure B-20).

**Figure B-20 File Manager Menu**

You can also access the File Manager using the Locations & Doors module. Select Locations & Doors from the Doors menu, and then select Gateway Controllers from the View menu. Expand a location tree and right-click a Gateway to select File Manager from the menu.

Step 5 Select the Image tab to display a list of the firmware images currently loaded on the Gateway module (Figure B-21).

**Figure B-21 File Manager Window: Image Tab**

Each row displays information about the firmware image:

• **Name:** the image filename.

• **Version:** the firmware version number.

• **Download Time:** the time and date when the image was downloaded to the Gateway module.
- **Active**: The Active image will become the Running image when the Gateway is reset. The image marked **Yes** is the active image on the Gateway.

- **Running**: The Running image is the image currently used to operate the Gateway. The image marked **Yes** is the current running image on the Gateway.

**Step 6** Download a new firmware image from a TFTP server, if necessary:

- Select the **Initiate Download** button, as shown in Figure B-21.
  
  The Initiate Download Input window appears, as shown in Figure B-22.

**Figure B-22 Initiate Download Input Window**

- Enter the **Image Name**:
  - If the image is located on the Cisco PAM TFTP server, click **Browse** (Figure B-22) to select a firmware image name.
  - If the image is located on a different TFTP server, enter the filename manually.

- Enter the **TFTP Server IP address**.
  
  The Cisco PAM appliance TFTP server IP address is entered by default.

- Enter the directory **Path** on the TFTP server for the firmware image.
  - Leave this field blank if using the default location for the built-in Cisco PAM appliance TFTP server.
  - Be sure the path and filename are valid. The administration tool does not verify remote server paths.

- Select the following options to define what will occur after the image is loaded to the Gateway:
  - **Set as active image**: (checked by default) make the firmware file new active image. The Active image is the firmware that will become the Running image when the Gateway is reset.
  - **Delete configuration**: delete the module configuration. The configuration is automatically reloaded when the module establishes communication with the Cisco PAM appliance.
  - **Delete events**: delete all events stored on the module.
- **Reset Gateway**: (checked by default) perform a soft reset to powercycle the module. Resetting the Gateway changes the Active image to the Running image. The Gateway will be down during the reset. Uncheck this box to reset the Gateways manually, as described in Step 9.

- **Reset time**: defines when the Gateway reset will occur. If this field is left blank, the Gateway resets immediately after the image is downloaded to the Gateway. You can also enter a time (in 24-hour notation) when the Gateway should reset. This field is used only if the Reset Gateway option is checked.

**Note**
See Select the Following Options When Upgrading Gateway Firmware, page B-3.

**Step 7**
Click **OK** to close the window and copy the firmware image to the Gateway module.

- Any actions selected in Step 6e are initiated. For example, the new active image is set and the Gateway module is reset (the Gateway must be reset to activate the new image).

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

**Step 8**
Click **Refresh** in the File Manager window to refresh the information and verify the Active and Running firmware image (see Figure B-23).

**Figure B-23  File Manager Window: Image Tab**

Each row displays the following information:

- **Name**: the image filename.
- **Version**: the firmware version number.
- **Download Time**: the time and date when the image was downloaded to the Gateway module.
- **Active**: The Active image will become the Running image when the Gateway is reset. The image marked **Yes** is the Active image on the Gateway.
- **Running**: The Running image is the image currently used to operate the Gateway. The image marked **Yes** is the current Running image on the Gateway.

f. (Optional) To change the active image, select an image and click the **Active Image** button. This button is available only if the selected file is not the active image. The Active image does not become the Running image until the Gateway is reset.

g. Click **Close** to accept the changes and close the window.
**Step 9** (Optional) Reset the Gateway.

This step is necessary if you did not select the option to **Reset Gateway** in Step 6e, or want to change the Running image. The **Active** image becomes the **Running** image only after the Gateway is reset.

To reset the Gateway, do the following:

a. In the **Hardware** module, right-click the Gateway controller (blue icon).

b. Select **Reset Gateway**, as shown in **Figure B-24**.

**Figure B-24**  **Reset Gateway Command**

![Reset Gateway Command](image-url)
Troubleshooting

If your Cisco PAM appliance is not working as expected, begin troubleshooting by following the procedures in this appendix. This appendix guides you through some initial checks and procedures that can help you solve some basic problems.

Contents

- Licensing: Frequently Asked Questions, page C-1

Licensing: Frequently Asked Questions

This section provides answers to common licensing questions. For more information, see Obtaining and Installing Optional Feature Licenses, page 2-21.

<table>
<thead>
<tr>
<th>Table C-1</th>
<th>Licensing: Frequently Asked Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>What does the CPAM base license cover?</td>
<td>The base license will permit the following number of modules (Cisco or non-Cisco) to connect to the CPAM server:</td>
</tr>
<tr>
<td></td>
<td>• Release 1.0.0: 4 modules are included with the base license</td>
</tr>
<tr>
<td></td>
<td>• Release 1.1.0 and later: 32 modules are included with the base license</td>
</tr>
<tr>
<td>What additional license SKUs are available for additional Cisco modules?</td>
<td>• CIAC-PAME-M64= is needed for up to 64 additional Cisco Modules</td>
</tr>
<tr>
<td></td>
<td>• CIAC-PAME-M128= is needed for up to 128 additional Cisco Modules</td>
</tr>
<tr>
<td></td>
<td>• CIAC-PAME-M512= is needed for up to 512 additional Cisco Modules</td>
</tr>
<tr>
<td></td>
<td>• CIAC-PAME-M1024= is needed for up to 1024 additional Cisco Modules</td>
</tr>
<tr>
<td>What do I need if I have 200 Cisco modules?</td>
<td>You need the base, plus quantity 2 of CIAC-PAME-128=</td>
</tr>
<tr>
<td>Are licenses cumulative?</td>
<td>Yes, if you currently have a 64 module license and need to add 50 more, you need quantity 1 of CIAC-PAME-64= to add to the current license.</td>
</tr>
</tbody>
</table>
### Licensing: Frequently Asked Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>How are licenses keyed to the specific server?</td>
<td>By the CPAM software serial number that is obtained using the CPAM admin web interface. The serial number is 16 digits in the range of 0-F. The server hardware serial number is not used.</td>
</tr>
<tr>
<td>If the CPAM is in an HA (high availability) configuration with two servers, do I need two copies of each license?</td>
<td>No, all licenses are installed on the primary server with the exception of the HA license. The HA license is the only license installed on the standby server.</td>
</tr>
<tr>
<td>What is the SKU for the HA feature?</td>
<td>CIAC-CPAME-HA= is the SKU for the HA license.</td>
</tr>
<tr>
<td>Can a license be moved to another CPAM server?</td>
<td>No, once a license is issued it is bound to the server serial number that the license is issued against. You must obtain a new license for the server you wish to move the license to.</td>
</tr>
<tr>
<td>Who handles licensing issues for the CPAM server?</td>
<td>TAC can assist with installing a license. TAC can not generate licenses. If you have a problem with the license file itself you can email <a href="mailto:licensing@cisco.com">licensing@cisco.com</a> and seek additional assistance. You should include the CPAM serial number and the purchase or sales order number as well.</td>
</tr>
</tbody>
</table>
| What software features require a license?                                | • The Badge Designer application requires SKU CIAC-BD=  
• The Enterprise Data Integration feature requires SKU CIAC-EDI= |
Table C-1  Licensing: Frequently Asked Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the process to acquire additional licenses?</td>
<td>Cisco or our partner generates a sales order and the licensing team then generates a PAK (Product Authorization Key). The PAK is entered into the Cisco.com licensing portal, and a license file is generated. The file can be downloaded at this point. The file is then installed onto the CPAM primary server (except the HA license which is installed on the standby server) using the web GUI interface.</td>
</tr>
<tr>
<td>What are Controller Conversion licenses for?</td>
<td>These are for supporting non Cisco access panels.</td>
</tr>
</tbody>
</table>
| What are the Controller Conversion licenses SKUs? | • CIAC-PAME-L64= is needed for up to 64 additional non-Cisco Modules  
• CIAC-PAME-L128= is needed for up to 128 additional non-Cisco Modules  
• CIAC-PAME-L512= is needed for up to 512 additional non-Cisco Modules  
• CIAC-PAME-L1024= is needed for up to 1024 additional non-Cisco Modules |

![Cisco PAM Server Administration](image)
Security

This appendix includes information used to ensure the security of your Cisco PAM appliance.

Contents

- Cisco PAM TCP Port Requirements for Firewall Connections, page D-1
- Related Security Documentation, page D-1
- Disabling the Cisco PAM TFTP Server, page D-2

Cisco PAM TCP Port Requirements for Firewall Connections

Table D-1 lists the TCP ports used by the Cisco PAM appliance. Cisco PAM desktop clients require access to these ports when connecting to a Cisco PAM appliance that is behind a firewall.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>HTTP for video and redirect to HTTPS</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>TCP 1236</td>
<td>Fixed port for CPAM client to server communications.</td>
</tr>
<tr>
<td>TCP 3306</td>
<td>MYSQL</td>
</tr>
<tr>
<td>TCP 8020</td>
<td>Default port for Gateway to Cisco PAM communication.</td>
</tr>
<tr>
<td>UDP 69</td>
<td>TFTP</td>
</tr>
</tbody>
</table>

Related Security Documentation

Refer to the following documentation for security information related to Cisco PAM.

- Red Hat Enterprise Linux 4.5.0 Security Guide
- Security in MySQL
Disabling the Cisco PAM TFTP Server

The Cisco PAM appliance includes a TFTP server that is enabled by default. This TFTP server is used primarily to store firmware images for upgrading Gateway modules, as described in Upgrading Gateway Firmware Images Using Cisco PAM, page B-18.

To disable the TFTP server, complete the following steps.

1. **Note** If the TFTP server is disabled, you must upgrade the Gateway firmware using image files stored on an external TFTP server. See Upgrading Gateway Firmware Images Using Cisco PAM, page B-18 for more information.

   **Step 1** Log in to the Cisco PAM Server Administration utility.
   See Logging on to the Cisco PAM Server Administration Utility, page 2-2.

   **Step 2** Select the Monitoring tab and then select Status.

   **Step 3** Verify that the TFTP Service is Up, click Stop, as shown in Figure D-1.

   **Step 4** After the confirmation message appears, verify that TFTP Service is Down.

   **Figure D-1** TFTP Service in “Up” State

   ![TFTP Service in “Up” State](image)

   **Tip** Once the TFTP Service is Down, the button changes to Start. Click Start to enable the TFTP server.
GLOSSARY

**A**

**Access level**  
A set of access points, each with a corresponding time schedule, that determine where and when a badge holder has permission to pass through an access point.

See also: Access point

**Access point**  
An access point is an access-controlled point such as a door, turnstile, or gate. At the hardware level, this consists of a grouping of devices:

Door Contact
Door Strike
Reader
REX

**ADA**  
ADA is an abbreviation for the Americans with Disabilities Act.

**ADA strike time**  
ADA strike time refers to the ability of Cisco Physical Access Manager to customize the time before the door strike locks a door after access granted. This can be used for badge holders who need more time entering and exiting access points.

**Alarm**  
An event that has been configured to be presented as an alarm to the operator. Alarms may be in different states indicated by color and/or blinking, and alarms may be acknowledged, cleared, and commented on by the operator. An alarm has an associated priority which indicates its severity or importance.

See also: Event

**Alarm State**  
The state of an alarm, based on operator actions. May be one of several states which also have an associated color and/or blinking:

*Active:* Blinking red. The alarm is new and has not been acknowledged or resolved in any way.

*Acknowledged:* Solid orange. An operator is aware of the alarm, but it has not been resolved.

*Cleared:* Solid green. The alarm has been resolved.

See also: Alarm

See also: Top alarm state

**APB**  
See also: Anti-passback
**Anti-passback**

A mode of operation that hinders a badge holder from entering an access point, then passing back their badge to another person to enter the same area. The consequences of violating the anti-passback conditions vary depending on the mode of anti-passback the individual access point is configured for.

See also: Area

**Anti-passback (APB) delay**

The time a badge holder must wait before they can reuse their badge at the same reader. This is not used for all APB modes.

See also: Anti-passback

See also: Anti-passback mode

**Anti-passback (APB) mode**

A mode which determines how anti-passback is enforced. The following is a list of possible modes.

- **Soft (grant access):** Will let the badge use the reader if the badge has an incorrect entry area, but reports the passback violation to the software.

- **Hard (deny access):** Will not let the badge use the reader if the badge has an incorrect entry area.

- **Reader-based using reader history:** Same badge cannot be used twice in a row at this reader within the delay time.

- **Reader-based using card history:** The badge cannot be used two consecutive times at this reader within the delay time, even if others use the reader.

- **Area-based:** Hard APB within delay, soft APB after delay time.

See also: Anti-passback

**Area**

When an access point is configured for APB, the access point has an associated entry area and exit area. These areas are used to track the badge holders location.

See also: Anti-passback

**Audit record**

A record of an operator modifying an object in the system, including the date, time, and the state of the object before and after the edit. An audit record is a type of event.

See also: Event

---

**B**

**Badge**

Also known as a card. A type of credential encoded with a card number, generally on a magnetic stripe or internally like a proximity card, and used to enter access points.

**Baud rate**

A measure of the rate at which a modem or serial connection transmits data. This is measured in bits per second (bps).

**Biometric**

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. A biometric in Cisco Physical Access Manager refers to a type of credential used for biometric verification.
C

Calendar  A calendar defines a set of holidays. The holidays within the calendars are then used in conjunction with access levels to control access during holiday periods.

Camera  Cameras record digital video files to be stored on the DVR.

See also: Closed Circuit Television

CAN (Controller Area Network) bus  A 3 wire parallel communication bus that runs between the Gateway and up to a total of 15 additional modules. These additional modules can be any combination of Reader, Input, or Output modules.

The distance limit on the CAN bus is 1320 feet. The last module on the CAN bus must be set to terminate the CAN bus.

Card  See Badge.

Card format  The bit structure of a particular card. The average card format includes the card number, facility code, and parity bits. The two types of card formats supported by Cisco Physical Access Manager are Wiegand and magstripe.

Card format type  The type of a card format, which may be Wiegand or magstripe.

See also: Wiegand

See also: Magnetic Stripe

Card number  The card number encoded within the badge, often on the magnetic stripe or internally for proximity cards.

See also: Badge

CCTV  Closed Circuit Television

CHUID/CUID  Card Holder Unique Identity Model.

Cisco PAM client  A Java applet that runs on a Windows client PC or workstation that is used to manage the Cisco PAM server and associate Gateways. It can be used to monitor the physical access system of sensors and locks. It can be used to configure the operation of the Cisco PAM server and the access modules.

Cisco PAM server  An appliance used to manage and monitor a physical access infrastructure comprised of Cisco Gateway, Reader, Input and Output modules. It can interact with corporate directories like LDAP or MS Active Directory to validate access credentials for user access badges. It also interacts with Cisco VSM to provide video for configured devices and events.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Closed Circuit Television</strong></td>
<td>A collection of surveillance cameras conducting video surveillance. Each camera is viewable on a monitor.</td>
</tr>
<tr>
<td><strong>Credential</strong></td>
<td>A general category that includes login, badge, and biometric; something that is used to gain access to a physical or logical resource.</td>
</tr>
<tr>
<td></td>
<td>See also: Login</td>
</tr>
<tr>
<td></td>
<td>See also: Badge</td>
</tr>
<tr>
<td></td>
<td>See also: Biometric</td>
</tr>
<tr>
<td><strong>Dashboard</strong></td>
<td>A module with real-time graphs, charts, and diagrams that is used for monitoring details and statistics for the system.</td>
</tr>
<tr>
<td><strong>Debounce</strong></td>
<td>Debounce is a parameter representing the number of consecutive scans that must be in agreement before changing the state of the input point. Debounce is used to prevent incorrect reads. Each scan period is 16.7 milliseconds. The recommended setting for a REX is 2 and 4-6 for standard inputs.</td>
</tr>
<tr>
<td></td>
<td>See also: Input point</td>
</tr>
<tr>
<td><strong>Dedicated Micros Driver</strong></td>
<td>A dedicated micros driver is a software device that manages the sending and receiving of data between the CCTV cameras and the DVR.</td>
</tr>
<tr>
<td></td>
<td>See also: Driver</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>In a network using subnets, the router that forwards traffic to a destination outside of the subnet of the transmitting device.</td>
</tr>
<tr>
<td></td>
<td>See also: Subnet</td>
</tr>
<tr>
<td><strong>Department</strong></td>
<td>A sub-division of an organization, and used to organize personnel.</td>
</tr>
<tr>
<td></td>
<td>See also: Organization</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>A hardware (and in some cases software) component in the system. Events are generally associated with a Device. Devices also can have different states with varying color and severity.</td>
</tr>
<tr>
<td><strong>Device Status</strong></td>
<td>The real-time status of a device. Examples include: Online, Offline, Unknown, Secure, and Alarm. Each state has an associated color and severity. Not to be confused with top alarm state, which depends on operator actions in the application. For example, if a door is forced open, and then shut again, the status will go from forced open to secure, but the top alarm state will reflect the forced open state until an operator clears it.</td>
</tr>
<tr>
<td></td>
<td>See also: Top Alarm State</td>
</tr>
<tr>
<td><strong>Device status module</strong></td>
<td>Allows operators to monitor the real-time status of all devices connected within the access-control. Operators can view the device properties, as well as status and the top alarm at any given device.</td>
</tr>
</tbody>
</table>
DHPC
Dynamic Host Configuration Protocol (DHCP). A network application that automatically assigns IP addresses to devices in the network.

The Cisco Physical Access Gateway can obtain an IP address via DHCP. DHCP options 150 and 151 can also be passed with the DHCP lease. These options point the Gateway module to the Cisco PAM server and TCP port to use for the Gateway to Cisco PAM server TCP/IP session. The Gateway can also have a static IP address. The Cisco PAM server should have a static IP address. The Reader, Input and Output modules do not require an IP address.

DIP switch
A set of small on-off switches mounted on hardware. The dip switches are used to configure settings on the hardware.

Door contact
A door contact is a device that monitors whether a door is open or closed. A door contact is part of an access point.

See also: Access point

Door strike
A door strike is a device that physically locks or unlocks the door. A door strike is part of an access point.

See also: Access point

Driver
A process on a host computer used to communicate between the host computer and hardware devices. Different types of supported hardware generally have different drivers.

Driver manager
A driver manager is a software device that manages all drivers in the system.

See also: Driver

Duress Request
This is a feature used by a badge holder under duress on a reader/keypad configured to accept PIN and Duress entries. If the badge holder enters their assigned PIN plus the configured duress key or keys, this will send a duress signal to the access-control system.

For example: Duress code is configured as 1 digit, and that is 5. An individual has a personal identification number of 1111. If that individual enters 11110 or 1111, no duress indication is sent to the access-control system. If the individual enters 11115 a duress indication will be sent to the access-control system.

In this example, any PIN entry of 1111x, where x is 0 through 4 or 6 though 9 will result in grant access with no duress signal. Only a PIN entry of 11115 will grant access with a duress signal. If the user enters 1111 only, the PIN entry timeout will have to expire and the individual will be granted access with no duress signal.

DVR
DVR is an abbreviation for digital video recorder. A DVR records video from CCTV cameras to disk. Allows for viewing of live or past video.

See also: CCTV
Encryption
A method of securing data so it cannot be read by unauthorized users or applications. The configuration file and card database located on the Gateway module are encrypted.
Cisco PAM backup files created by the backup process are encrypted with a password. The password used when creating the backup file must be entered when using the file for a restore operation.

Event
An activity within the system, recorded to the database, and available for monitoring or reporting.

Event Policy Manager
A module used to configure the way events are processed and displayed. The following attributes can be configured:

- Is alarm: This determines whether the event is an event or alarm.
- Is recorded: This determines whether the event is recorded. If the event is not recorded, it cannot be an alarm.
- Priority: This determines the priority of the event or alarm.
- Alert sound: The sound to be played when the event occurs.

See also: Event

Facility code
A segment of bits encoded on a card which represent a number in association with a facility. Often all cards issued for a single facility will have the same facility code.

Fail-Safe lock
A lock that requires voltage to remain in the locked state. If voltage is removed, the lock will move to the unlocked state.

Fail-Secure lock
A lock that does not require voltage to remain in the locked state. If voltage is removed, the lock remains in the locked state.

FASC-N
Federal Agency Smart Card Number.

Filter
A tool allowing operators to select which objects should be displayed.

FIN
Foreign Identification Number. Used as an alternative to Social Security Number (SSN).
<table>
<thead>
<tr>
<th><strong>H</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>See Device</td>
</tr>
<tr>
<td><strong>Hardware module</strong></td>
<td>A module allowing operators to add, edit, and disable the hardware.</td>
</tr>
<tr>
<td></td>
<td>See also: Device</td>
</tr>
<tr>
<td><strong>Hardware tree</strong></td>
<td>The hardware tree is a hierarchical display of all devices in the system, seen in the Hardware module and the graphic maps editor. Each device in the hardware tree can be expanded or collapsed to show or hide its sub-devices by clicking the + or - to its left.</td>
</tr>
<tr>
<td></td>
<td>See also: Device</td>
</tr>
<tr>
<td></td>
<td>See also: Hardware tree</td>
</tr>
<tr>
<td></td>
<td>See also: Hardware module</td>
</tr>
<tr>
<td><strong>Hexadecimal</strong></td>
<td>A numbering system usually written using the symbols 0–9 and A–F or a–f.</td>
</tr>
<tr>
<td><strong>HID</strong></td>
<td>A company manufacturing the industry standard proximity access-control cards.</td>
</tr>
<tr>
<td></td>
<td>See also: Proximity</td>
</tr>
<tr>
<td><strong>Hold time</strong></td>
<td>The amount of time in seconds that the system will ignore an active state of a monitor point. The system will hold a higher priority status before a lower priority status is reported. As an example, motion detectors can sometimes trigger multiple times per second causing the Event logs to fill unnecessarily fast with useless data.</td>
</tr>
</tbody>
</table>
Hot stamp

The number physically printed or embossed on a badge. This number is generally independent of the Card Number. Not all badges have a hot stamp number.

See also: Badge

HSPD-12


HTTPS

Hypertext Transfer Protocol Secure. A combination of the Hypertext Transfer Protocol and a network security protocol. Gateway and Cisco PAM HTTP access is via HTTPS.

See also SSL.

I

input

A sensor that has 2 states, open or closed. The steady state can either be normally open (NO) or normally closed (NC). When moved to the non-steady state, the input is used to make a decision. Typical input is a door sensor. It is used to determine if the door is in the opened or closed position. An input has 2 pins marked + and -, Gateway, Reader, and Input module inputs can be supervised or un-supervised. See also Supervised input.

Inputs do not require power. Power is supplied from the module.

Input module

A device that can accept 10 inputs. It communicates with the CPAM server via the CAN bus and the Gateway module. The module requires an external 12V to 24V DC source and can not be powered via POE.

IP address

The Internet Protocol address. The Cisco Physical Access Gateway can obtain an IP address via DHCP. DHCP options 150 and 151 can also be passed with the DHCP lease. These options point the Gateway module to the Cisco PAM server and TCP port to use for the Gateway to Cisco PAM server TCP/IP session. The Gateway can also have a static IP address. The Cisco PAM server should have a static IP address. The Reader, Input and Output modules do not require an IP address.

LDAP

LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.

LED

Light-emitting diode. A semiconductor diode that converts applied voltage to light. LEDs are used to display status, communication, and other information on various devices.

Localhost

Default hostname describing the local computer address.

Login

A credential used to obtain access to the application as an operator. A login has a username and password, along with a set of profiles which determine what the operator has access to within the application. See also: Profile

Logins module

A module used to manage operator logins in the application. See also: Login
MAC Address

MAC address is an abbreviation for Media Access Control address that uniquely identifies each node of a network. Each type of network medium requires a different MAC address.

Magnetic Stripe

A strip of magnetic recording material on which certain data is stored. See also: Card Format Type and Wiegand

Masked

A hardware state for monitor points and access points where one or more active conditions will be reported to the software as masked.

Module

An independent section of Cisco Physical Access Manager with some distinct function.

Monitor point

A monitor point is an input on a sub-controller that is configured to monitor an external device or signal, typically an alarm input.

Monitor point group

MPG is an abbreviation for monitor point group. A MPG is an operator defined organization of access points and monitor points. Commands issued to the MPG influence all of the contained devices. A total of 128 monitor points or 64 access points can be included in a MPG. One access point counts for two monitor points.

Multiplexer

A type of hardware which can combine multiple communication channels into a single communications channel.

Output

A device that requires a trigger to change state. The steady state is either normally open (NO) or normally closed (NC). Once a decision is made for the device to change state, the module output interface will open or close a relay to trigger the device. A typical output device is an electric-mechanical door lock. IE: When not triggered, the lock is in the 'locked' position. When triggered by the output module, the lock moves to the 'unlocked' position.

Outputs generally require power, and the output module will either close or open a relay to trigger the device. The power to drive the device should be inline with the relay on the output module. The output relay on the module has 3 pins marked NC, C and NO. NC is normally closed, C is common or ground and NO is normally open. Exception might be for a POE capable lock, where the power for the lock is obtained from the Reader attachment of a Gateway or reader module.

Output module

A device that can drive 8 outputs. It communicates with the Cisco PAM server via the CAN bus and the Gateway module. The module requires an external 12V to 24V DC source and cannot be powered via POE.

Organization

An organization with which a personnel record can be associated.

PDF

Portable Document Format. A document format defined by Adobe, which represents a printable/viewable document in a manner that is independent of the original system used to create it. Viewing PDF documents requires the Adobe Reader, freely available at www.adobe.com.
Personnel module  A module used to manage personnel information.

PF input  This input is used to detect a power failure. If activated, an alarm is posted notifying the administrators that a device has lost power. The PF input has 2 pins marked + and -. This input can be re-allocated to act as an unsupervised input.

PIN  Personal Identification Number. A badge has a PIN associated with it, which, depending on the configuration of an access point, is entered into the keypad on the access point's reader.

POE  Cisco Power Over Ethernet. This provides up to 15.4 watts to power devices attached via a CAT5 cable to a POE capable switch.

Power Over Ethernet  See POE.

Privilege  Privileges define what a credential has access to. Examples of privileges include access levels and profiles.

See also: Credential

See also: Profile

See also: Access level

Profile  A profile determines the software modules and the commands that an operator has access to upon logging in.

Profiles module  A module for managing profiles. See also: Profile

Proximity  A technology where the presence of a certain object can be sensed by a device without having direct contact. See also: HID

R

Reader  A reader is a device for receiving a card number and/or PIN from a badge holder.

Reader module  A device that can accept one 10 wire Weigand reader, or two 5 wire Weigand readers, three inputs, three outputs, power fail, and tamper sensor inputs. It requires a Gateway module to facilitate communication with a CPAM server. The module requires an external 12V to 24V DC source and can not be powered via POE.

Relay  A device that responds to a small current or voltage change by activating switches or other devices in an electric circuit.

REX device  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. When a door state changes from closed to open, it means someone has unlocked the door from the secure side. If the door state moves from closed to open, with no valid reader swipe or REX activation, it can indicate that the door was forced open.

A REX is part of an access point. See also: Access point.

RTS mode  A method of hardware flow control used in serial communications.
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scroll lock</strong></td>
<td>A tool button in some modules that allows the operator to stop the scrolling of items in the window. New items will continue to be added to the window, but the window will not automatically scroll to show the most recently added item.</td>
</tr>
<tr>
<td><strong>Serial communications</strong></td>
<td>A method of communicating over a dedicated line.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>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 Physical Access Manager only have a single database, and hence a single site. Multiple sites are used in larger configurations, for example a company with offices around the world, with a Cisco PAM database at each office.</td>
</tr>
<tr>
<td><strong>SSN</strong></td>
<td>Social Security Number. A nine-digit number issued to individuals by the U.S. government for tax purposes, and often used as an identification number.</td>
</tr>
<tr>
<td><strong>SSL</strong></td>
<td>Secure Sockets Layer. A security protocol for secure connections using over the internet. Gateway to Cisco PAM server can utilize SSL for the connection. All gateways and Cisco PAM server must be configured for SSL, or for no SSL. A mix of SSL and non-SSL is not supported. Gateway and Cisco PAM HTTP access is via HTTPS. See also HTTPS.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>See Device Status</td>
</tr>
<tr>
<td><strong>Subnet</strong></td>
<td>A portion of a network, which shares a common network address with other portions of the network and is distinguished by a subnet number. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100 would be part of the same subnet.</td>
</tr>
<tr>
<td><strong>Supervised input</strong></td>
<td>A supervised input has 4 states. (1) Short (2) Open (3) Non-Alarm or (4) Alarm. Supervised inputs require two 1K resistors in the circuit for detection of Short and Open states. See also input and Input module.</td>
</tr>
<tr>
<td><strong>Supervised input</strong></td>
<td>An unsupervised input has 2 states. (1) Normal or (2) Alarm.</td>
</tr>
<tr>
<td><strong>TCP/IP communications</strong></td>
<td>A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.</td>
</tr>
<tr>
<td><strong>Telnet</strong></td>
<td>An Internet communications protocol that enables a computer to function as a terminal working from a remote computer.</td>
</tr>
<tr>
<td><strong>Time interval</strong></td>
<td>A period of time defined using a start time and time. Each period has a list of days of the week (Sun. through Sat.) and holidays of when it can be active.</td>
</tr>
<tr>
<td><strong>Time received</strong></td>
<td>The time an event or alarm was actually received by the access-control system and stored in the database.</td>
</tr>
</tbody>
</table>
**Time schedule**
A defined set of time intervals used to make access-control, triggering, and other decisions. See also: Time interval

**Time zone**
24 longitudinal divisions of the globe, nominally 15 degrees wide, in which clocks show the same time.

**TM input**
This input is used to detect if a component box is being tampered with. It acts like a normal input and would be in the normally closed position indicating that the component box access door is closed. Once opened, this input would alert and administrator that the component access door is, or was, opened. The TM input has 2 pins marked + and -. This input can be re-allocated to act as an unsupervised input.

**Top alarm**
The most important alarm present at a given device. Based on alarm state, time, and priority. See also: Alarm and Alarm state

**Top alarm state**
The state of the top alarm at a given device. Possible states include active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity. Not to be confused with device status, which is independent of operator actions in the application. For example, if a door is forced open, and then shut again, the status will go from forced open to secure, but the top alarm state will reflect the forced open state until an operator clears it. See also: Device Status and Alarm state

**Trigger**
A trigger waits for an operator-defined combination of events, addresses, properties, and time schedules to occur, then executes a procedure. See also: Procedure

**TTR**
Triple Technology Reader. A reader which combines three devices in one: a magnetic card reader, HID proximity card reader, and piezoelectric keypad.

**U**

**Use limit**
An option which can restrict a badge to a certain number of uses. The default is 0 (off). See also: Badge

**Username**
A sequence of characters used as identification when logging onto the application.

**V**

**View query**
An option within the filter tools, giving operators the capability to view the actual filter definition as an SQL-like expression string. See also: Filter

**VIN pins**
Voltage input. This is where you can use +12 to +24 volts DC to power the module.

**W**

**Wiegand card format**
Wiegand card format stores card data using binary values. The information includes parity error detection, facility code and the card ID. Each card has a particular format that must be configured in the access-control panel to permit the panel to correctly interpret the card data. A very common Wiegand card format is a 26 bit format, with the first and last bit for parity, 8 bits for the facility code and 16 bits for the card number.

When configuring the Credential Template on the Cisco PAM server you must configure it to match the card format for the reader. The format might be more or less than 26-34 bits.
**Weigand Interface**

This is a 10 pin interface on the Gateway or Reader module used to attach a card reader. The 10 pin interface can be logically configured to operate as two 5 wire Weigand interfaces to support two readers. When run in 5 pin mode, the LED function on the reader is not used.

The minimum leads needed for the Weigand reader to work are:

- PWR = Power
- GND = Ground
- D0 = Data bit 0
- D1/clock = Data bit 1 and the clock
- GRN = LED power
- DRTN = Data return (1 end only)

**Wizard**

An interactive utility that guides an operator through potentially complex tasks, including adding and configuring a new sub-controller.